

UNCORRECTED SAMPLE CHAPTER
I.T. APPLICATIONS VCE UNITS 3 AND 4 STUDENT BOOK
3RD EDITION
ISBN: 9780170187473
SEC 7886

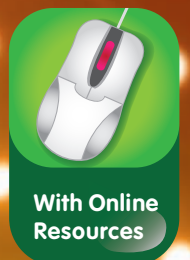


Customer Service: 1300 790 853
www.nelsonsecondary.com.au

I.T. applications

vce units 3&4 third edition

series editors Colin Potts James Lawson
Therese Keane Margaret Lawson



Contents

Preface	iv
Outcomes grid	vii
About the authors	x
<hr/>	
Unit 3	
Introduction to Unit 3	1
1 Networks	2
2 Online communities	53
Preparing for Unit 3 Learning Outcome 1	95
3 Data management tools	97
Preparing for Unit 3 Learning Outcome 2	136
<hr/>	
Unit 4	
Introduction to Unit 4	139
4 Organisations and information needs	140
5 Developing a solution using database software	177
6 Developing a solution using spreadsheet software	216
Feature: User documentation	246
Preparing for Unit 4 Learning Outcome 1	266
7 Information management	268
8 Security and ethical considerations	312
Preparing for Unit 4 Learning Outcome 2	355
<hr/>	
Acknowledgements	xx
Index	xx



Unit 3

Introduction to Unit 3

2-3 pars of text – still to come.

Outcome 1

1-2 pars of text – still to come.

Outcome 2

1-2 pars of text – still to come.

Chapter 1

Networks

Key knowledge

After completing this chapter, you will be able to demonstrate knowledge of:

- types of networks
- functions of key hardware and software components that support networks
- network operating systems and web server software
- types of communication technology
- network protocols
- security issues relating to networks
- types, purposes and functionality of websites that support information exchange within online communities
- types and characteristics of hardware and cross-platform software that support websites.

For the student

Networks are an important part of modern information systems. A network connection device is built into nearly every modern computing device. This chapter considers what a network does and some of the benefits derived from using networks. Following this is a section containing information about how networks operate and how they are arranged. It is useful to have some understanding of these concepts when interacting with network technicians and operators. Finally, we look at websites that support information exchange within online communities.

For the teacher

Networks are an integral part of everyday computer use, and some understanding of their operation, construction, components and topologies can benefit users in an organisation. Many information systems rely on networks to move data from one point to another and use networks to share resources.

Students are required to investigate the types of websites that support information exchange between online communities. In this chapter we look at wikis, blogs, forums and social networking sites. As technology changes, the relevance of different types of websites can alter. A list of approved website types will be published annually by the Victorian Curriculum and Assessment Authority in the VCAA Bulletin. Teachers are advised to check this list.

Teachers should also note that there is some overlap in the Information Technology Study Design's Key Knowledge that has resulted in some material being covered in both Chapter 2 of *Information Technology VCE Units 1 & 2* and this chapter of *IT Applications VCE Units 3 & 4*. Where possible, the content of this chapter probes a little deeper than that in Units 1 & 2. The considerable number of students who study the Units 3 & 4 course without having completed the Units 1 & 2 course warrants the inclusion of previously covered material. Teachers should use their discretion in terms of the emphasis they place on some sections of this chapter in light of their students' previous experience.

This chapter, together with Chapter 2, will assist students to complete Unit 3 Outcome 1, which requires students to create a prototype website that meets an online community's needs, and explain the technical requirements to support the hosting of this website.

Networks

Networks are widely used to share knowledge and resources. Many networks operate within a business or organisation, such as a school. Other networks can be very large, connecting computers in different suburbs, states or even countries. The **Internet** is a global network that consists of a worldwide collection of networks that connects millions of individuals, organisations, educational institutions, businesses and government agencies. In this chapter we will first consider what constitutes a network and the functions of the key hardware and software components of the network. We will then look at how websites can be set up on servers to allow online communities to share information.

Knowledge of how networks operate and can be used to enable the sharing of files and applications, the sending and receiving of communications and the sharing of resources will help us to understand how information systems can support decision-making and knowledge sharing.

What is a network?

A **network** connects computers together so that they can share data, information and **resources** such as printers, plotters, Internet access, servers, modems and scanners. A network connection allows your computer to communicate with other **devices** – to send messages, instructions and files, and to receive messages and files. The network has its own operating system so that it can control communication (usually called **network traffic**), handle **conflicts** (when two devices send messages at the same time) and run smoothly.

Networks are making the use of computers easier and more accessible for users at work, at home and in leisure activities. These days, very few people use non-networked computers in a work or leisure environment. Networks have made staying in touch via email or social networking sites a simple process.

When a user's computer is connected to a network, they are said to be online.

Think about IT 1-1

- 1 List some resources, other than printers and scanners, that can be shared on a network. Why are they called resources? How many people can share the same resource? Why does this vary depending on the resource?
- 2 Why are the printers on a network so much better (and faster) than the printers you might have at home? How many people share the colour laser printer in your school? How many people share the Internet connection?

Social networking sites are websites that allow users to exchange information, photos and videos. They include Facebook, Twitter, Flickr, MySpace, LinkedIn and YouTube.

Most social networking sites were established by individuals or small interest groups. Their popularity has seen them taken over by big corporations interested in their online advertising potential.

- Microsoft has a small investment in Facebook.
- Yahoo! owns the photo-sharing site Flickr.
- Google owns YouTube.
- News Corporation owns MySpace and Photobucket.
- TimeWarner owns Bebo, the third most popular social networking site after MySpace and Facebook.

Real time means there is no delay between sending and receiving a response – such as in a face-to-face conversation.

The home context is where most people will see the advantages of networking over the next few years. Businesses have already made significant use of the advantages offered by networking.

Think about IT 1-2

As a group, maintain a log over the next 10 days of when your classroom printer is actually printing, and create a spreadsheet showing times, averages, the longest continuous run, the longest run in which the printer was idle for less than three minutes between print jobs, the average usage in a school day, average usage over 24 hours, and average usage over seven days (including weekends). Also predict average usage when school holidays are included.

Note that printing needs are different in different subjects. Perhaps members of the class could maintain the log in all classes for which they are in the computer room.

Does this log give you some ideas about why there are so few printers in your school?

Advantages of networks

A network makes it easier to communicate between computers. For example, email users use the Internet to exchange ideas, information and files. Using a network for communication is much faster than sending a letter by traditional mail.

Before the World Wide Web was established, the primary use of networks was to save money by sharing resources. This is still an important aspect of their use today. The Internet is an example of a network that is used for communication and information or data sharing.

A network in a school allows a teacher to place files on a web server that students can download. Through the network, students have immediate access to the documents. The alternative is to print, photocopy, collate, staple and hand out the same document – a very time-consuming process.

Networks allow groups of people to work on the same project at the same time. By using **groupware**, they can almost instantly see changes made by others and respond to them in **real time**.

In general terms, the advantages of using a network are in resource sharing, accessing remote services, facilitating communications and sharing data and information.

Resource sharing

Resources such as printers (especially colour laser printers and plotters), scanners and Internet connections are too expensive to be connected to every computer within an organisation, and often are not used enough by a single user to justify the expense. If the computers and resources are connected via a network, the users of the network can access those resources when they are needed. Networks save money because a single resource can be shared between many users. Software programs used by an organisation can also be shared over a network, with considerable savings in costs. Several examples of resource sharing are described below.

Internet connection

Because of the expense of Internet connections, organisations are only willing to spend money where the benefits produced outweigh the costs involved. The convenience of having everyone connected to the Internet continuously but only having to pay for a single connection, can be considerable in an organisation that uses the web extensively or that requires constant external communication through email or webpages.

The quality of the connection needs to be higher where there are many users, but this will still be cheaper than providing everyone with their own connection.

Printing

Look around your computer room. There is probably only one good black and white laser printer and (if you are lucky) perhaps a colour laser printer. Before 1990 there would probably have been three or four printers connected to individual computers. If you wanted to print, you had to save to a floppy disk and walk over to a computer connected to a printer, load

up your disk, open your file and then print out the document. This was often called ‘sneaker net’.

This method is certainly inefficient by today’s standards. Consider how often a printer is actually printing onto paper. In most classrooms, it is printing for significantly less than 20 minutes an hour, so it is more efficient to share it among many users. This means that users sometimes have to wait for the resource, but usually the cost savings outweigh the minor inconvenience.

The benefit of enabling everyone to print from their own desk without having to go to a designated computer to print means that they can do more work. Many organisations rely extensively on printing, so networks can contribute significant cost savings.

Specialised printing jobs, such as engineering drawings and architectural plans, require plotters or extremely large and expensive inkjet printers. In a small- to medium-sized engineering business, for example, there would most likely only be one plotter. Allowing all users to access this plotter through a network reduces the need for additional plotters and hence means considerable savings in equipment purchases.

Software

Most software manufacturers offer network licences for their products. A **site licence** allows multiple users within an organisation to simultaneously use a software package. A site licence is usually less expensive than the equivalent number of stand-alone licences that would be required to provide the same service (Figure 1-1). The network administrator is able to closely control the software running over a network, such as the number of

The screenshot shows the Computelec website with a blue header and navigation bar. The main content area features a 'Latest News' section on the left and a 'Latest Promotions' section on the right. The promotion for Adobe Creative Suite 4 Design Premium includes a 40% discount on K-12 site licenses and lists the included software: Adobe InDesign CS4, Adobe Photoshop CS4 Extended, Adobe Illustrator CS4, Adobe Flash CS4 Professional, Adobe Dreamweaver CS4, Adobe Fireworks CS4, and Adobe Acrobat 9 Pro. It also mentions a free Total Training DVD set.

FIGURE 1-1

Schools can purchase a site licence to run a suite of software over a network.

A network-attached storage (NAS) device provides file-based data storage to other devices connected to the network. Although they are technically a computer in their own right, they do not have a keyboard or display, and are controlled and configured over a network, usually through a browser. They are commonly used to provide files to Xbox devices and games consoles.

Many pharmacies in Victoria order directly from their chain warehouse on a daily basis by dialling into the head office network, being authenticated, sending the order and then disconnecting.

A B2B network often will involve an extranet. An extranet is a private network that operates using Internet protocols and the public telephone system. It allows businesses to network with suppliers, vendors, partners, customers or other businesses, to share information or services. An extranet can be considered as part of a company's intranet that is extended to users outside the company, normally over the Internet.

Validation is the process of checking data for accuracy and reasonableness. It can be performed manually (for example, scanning data by eye to check that the current year is entered on a form) or electronically (using rules or formulas to check that the data lies within an allowed range). We discuss validation in greater detail in Chapter 3.

Electronic funds transfer point of sale (EFTPOS) is a device by which sales transactions can be directly debited to a customer's bank account at the point of sale through the use of a debit card.

On the first day of January 2010, the Bank of Queensland's EFTPOS card-processing system crashed. The system automatically incremented the year on New Year's Day, but jumped the date from 2009 to 2016 instead of 2010. This led to payments being rejected at the point of sale outlets of the bank's clients, since customers' credit and debit cards were due to expire before the incorrect date on the bank's computer system. The glitch was fixed five days later, but merchants had to rely on a manual transaction-processing system for several days.

users of a software package and which programs are installed. In this way, the organisation can avoid breaching licence agreements.

Other resources

Other resources that can be directly connected to the network or shared through connection to a computer include network-attached storage (NAS) servers, fax machines, network storage and directory services. These also offer benefits and savings.

Remote services

Remote services for customers, such as ordering through the Internet or in a business-to-business (B2B) situation (where businesses are connected directly to a part of the network of another business), can reduce costs for an organisation and improve the accuracy of their data processing. For example, an online sales company requires the customer to enter and check the order data. Staff are not involved in the data entry and thus transcription errors do not occur as the data is not changed after entry by the customer.

If there are no software errors, the order will be processed by the orders received department exactly as the client wanted. The customers have control of the data entry portion of their order and can get immediate feedback on **validation** processes when their order is entered in the system. Reducing opportunities for human error will allow an organisation to achieve its aim of improving the accuracy of its output and possibly reduce its staffing needs.

Automatic teller machines (ATMs) are an example of a remote service provided by banks. When a person enters instructions on an ATM, they are interacting directly with the bank's main computer. The ATM is a remote part of the bank's information systems.

Users connected to a network can move money from one bank account to another by means of electronic funds transfer (EFT) and an appropriate transmission media (Figure 1-2).



FIGURE 1-2

Using electronic funds transfer to purchase groceries is an example of using a remote network service. The customer is able to authorise direct payment from their bank account using an EFTPOS terminal to connect to the bank's server, usually by telephone line.

Issue

The speed of EFTPOS

The mainframe computer in a bank is a very powerful machine, capable of processing transactions very quickly. Yet it can seem to take a long time before the ATM or EFTPOS machine responds to your request for money.

The delayed response time is not caused by the length of time it takes to retrieve your details from the bank's files; that takes about 10–20 milliseconds. The delay is because the bank only has one operating mainframe computer to process all its transactions, so that there can be no confusion over accounts and all processing is centralised. (Think about backup!) The computer has multiple processors to enable fast processing. Consider the sheer volume of transactions to be processed by one of the big banks in any minute during the day. If each of them requires access to the data stores (taking 10–20 milliseconds), the computer is going to be spending a long time just waiting for the data to be retrieved. The mainframe, therefore, uses a technique called **timesharing**, in which the processor spends a limited amount of time working on your task.

At the end of that time slice (often about 1–2 milliseconds), it unloads your job and does the next one. It cycles through all of the current jobs, giving each of them a small slice of processor time. When the processor is working at 800 megahertz (MHz), it is processing 800 000 000 instructions per second. If your job has a time slice of one millisecond, then it has the opportunity for 800 000 instructions to be completed in that time. Some time is spent loading and unloading the job, but that accounts for comparatively little time. If there are only 1000 jobs to do and each one has a time slice of one millisecond, the computer will return to your job in just one second. When it takes longer to return to your job, it is because there are more jobs waiting. At peak times during the day, there can be more than 30 000 jobs being processed at once.

Think about IT 1-3

- 1 Centralising all processing makes backup very simple. What are the implications if something goes wrong with the system?
- 2 Even before the banks implemented high charges for over-the-counter transactions, it was common to see long queues at the ATMs while tellers inside the bank had no customers. Why do you think that was the case?
- 3 How long are people prepared to wait when withdrawing money? Does the convenience of having access to cash 24 hours a day, seven days a week, outweigh the time spent waiting for a transaction to be processed?

Think about IT 1-4

List at least five ways in which a network at home could be an advantage for you. Explain why these are advantages to you personally.

Data and information sharing in organisations

A significant benefit provided by networks is the ability to share data and information. Files stored on any computer on a network can be accessed by any other computer on the network, provided access rights have been granted. Organisations often have large numbers of documents stored on a network and vital information held in databases that are required on a regular basis by employees. Being able to access this information via a network ensures that it is available promptly and that it is accurate. Since all users access the same files over a network, keeping information current is simply a matter of updating the network version of a document or file.

The network allows data to be shared between users and enables users to retrieve information from more than one source.

In a large school, the data relating to the allocation of students to classes is likely to be shared by the timetabler, the year level coordinators and the finance manager. When a network is used, the information produced by each of these users can be shared with other teachers and administration

staff, all with a minimum of fuss. Without a network, all of these people would require their own copy of the data, which, of course, would soon fall out of synchronisation and cause massive data duplication problems. **Synchronising** the data is the process by which all users ensure that they have the same data set and that it is up-to-date.

Data duplication occurs when two or more users have a copy of the data set and are working on it at the same time, instead of there only being one copy that is passed on to the next user as each person finishes with it. To prevent data duplication without a network, each person would have to give a copy of the updated data to all the other users as soon as they have made any changes to it. For example, if a student changes address, the office staff need to know, so they can change the address details of the student; the finance manager needs to know before sending out any accounts; and the coordinators need to know in case they wish to contact the student's parents. In the absence of a network, the school would have to invest considerable effort in sharing the information that is produced and it would be difficult to keep it all timely.

Facilitating communications

A network allows people to communicate easily within an organisation or with people outside the organisation through the use of the Internet. Email, chat rooms, messaging, telephony and videoconferencing are examples of communications available through a network.

A network improves communication between users because it becomes simpler and faster. Contrast email with the traditional postal service. With email, it is no trouble to ask a quick question and receive a fast response. Consider also the advantages of a chat program – communication is nearly instantaneous and difficulties can be resolved in real time.

Types of networks

Networks are established in many places, ranging from big and small businesses through to schools and ordinary homes. There are many other networks around us – some of which are not immediately apparent. Cable TV is a network on which the traffic is just one way. The telephone system is a network on which two-way traffic occurs. Mobile phones are part of another network, one using radio waves rather than wires or cables (Figure 1-3). The radio waves only travel a short distance to a local tower. The signal is then carried over cables to another phone, or a tower from which it can be broadcast to another mobile phone.

In this section, we will consider the types and arrangements of networks that are used in many organisations.

Network categories

On a network, computers and other devices are able to use a physical or wireless connection to share resources or exchange information. Depending on how the machines are connected, the network is categorised as either a local area network (LAN) or a wide area network (WAN). These are two significantly different network structures.

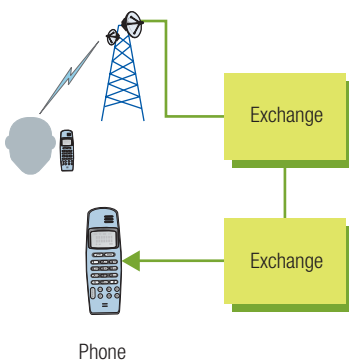
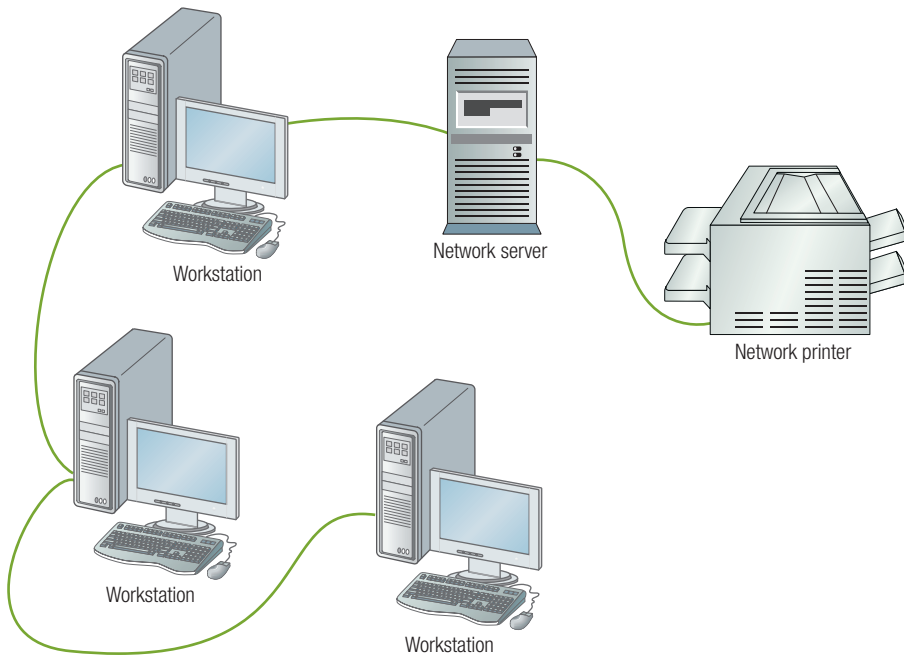


FIGURE 1-3

A mobile phone network

**FIGURE 1-4**

A local area network. Network nodes include workstations, printers and servers.

Local area network

A **local area network** is a network that connects computers and devices within close geographical proximity, such as within an office building, university campus, school or home. Traditionally, a local area network has been easily identifiable as those computers and devices that are connected by one set of cables within a given physical location. The advent of wireless technology has meant that computers that are located beyond the confines of a building may now form part of the LAN. Each computer or device on a LAN, called a **node**, is able to share resources, communicate, access remote services and share files (Figure 1-4).

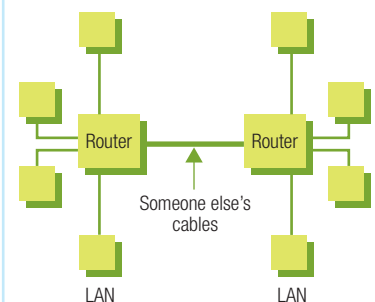
A **wireless LAN** uses radio waves, satellite communications, microwave or infra-red media to transmit signals between nodes. A wireless LAN often includes cabling that connects the wireless components to a wired network, to allow faster access to shared resources.

Wide area network

A **wide area network** is one in which communications are carried by a medium owned by someone who is not a part of the organisation whose data is being transmitted (Figure 1-5). So when a company uses telephone lines to connect two LANs, the two LANs together become a WAN. Transmission media can include microwave, fibre-optic cable, telephone lines and satellites.

WANs can be divided into different categories. These can include:

- a metropolitan area network that covers a single city
- a statewide network that can cover an entire state
- a national area network
- a worldwide network, such as the Internet.

**FIGURE 1-5**

A wide area network

Two libraries, one in the northern suburbs of Melbourne, the other in a southern suburb, may wish to share their book catalogue information. To achieve this, they could make use of a wide area network in which a computer at each library would be linked by a dedicated telephone line intended solely to carry their data.

The server specifications are likely to be equal to, or better than, the following: memory, 4 gigabytes; CPU speed, 2.4 gigahertz (GHz); storage, two 500 GB HDD.

A server with the above specifications would be suitable for a small business. The price of this server is about \$1800, with Windows Server 2008 Standard version network software costing a little under \$1000 (www.computeralliance.com.au). The price of a server depends on its specifications, which in turn are dependent on the function it is to perform. Factors that impact on server price include the number and type of processor (Intel Xeon, AMD Opteron), the maximum supported RAM (up to 64 GB) and the form factor (rack mountable, tower or blade). Highly configured Hewlett-Packard and Cisco servers can cost \$40 000 or more.

All of the above are WANs because the separate local networks communicate with each other using communication channels owned or managed by someone else.

Network architecture

The design of a computer network is called the **network architecture**. It includes the ways in which computers, devices and transmission media are connected. Three categories of network architecture are considered below: client–server, peer-to-peer and Internet peer-to-peer. The first two mainly apply to LANs, while an Internet peer-to-peer network would be based on a WAN.

Client–server network

Most networks are configured into a **client–server network** (Figure 1-6). A **client** is a machine that requests data or files. A **server** shares or sends data and files to those clients on the network who ask for them (usually the server will only send to those users that it has authenticated as being entitled to that material). Clients do *not* share/send files or data except to servers. In the **client–server** system, only the machines that are designated as servers are allowed to serve out data or files to other machines (which are set up as clients). A server can have many clients. The clients can request data from any server on the network that recognises them. Some servers are configured to only serve clients that they have authenticated (such as the print server in a school network), while others will serve data to any device that asks for it correctly (such as a public web server). **Print servers** accept print files and then serve them out to printers. A **mail server** accepts email for its own accounts from any other mail server (usually via the Internet), and accepts mail for sending from any authenticated account holder who is directly connected to it.

A server is designed and built to handle tasks considerably faster than an ordinary desktop computer. Thus a client–server network must have at

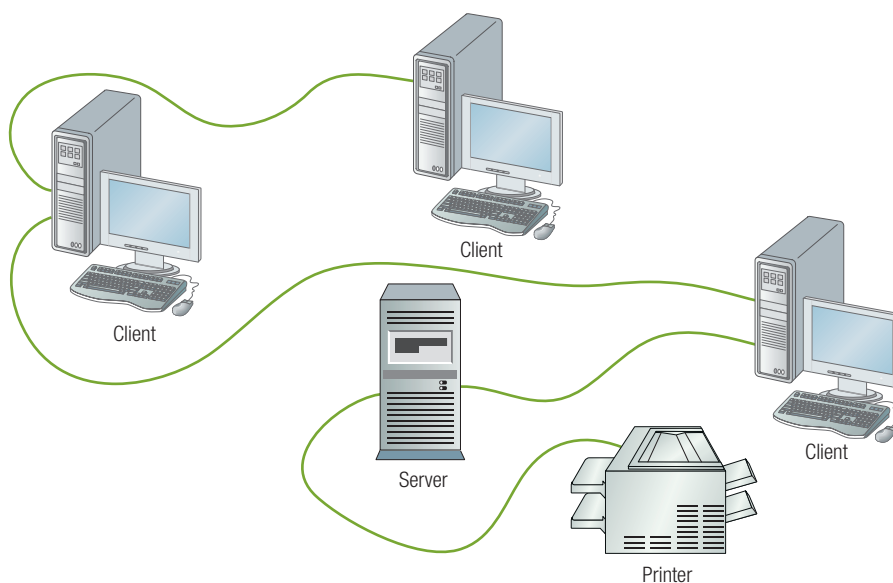


FIGURE 1-6

On a client–server network, one or more computers act as a server, and the clients access the server.

least one powerful machine that acts as a server and is not available to be used as a **workstation** (a client computer at which a user can work).

Server machines are generally considerably more expensive than client machines, but the resulting efficiencies of time and effort brought about by having a server usually make up for the increased cost.

Servers are designed to enable fast delivery of material from the server's hard drive to the network and to process requests quickly. All server software is **multi-tasking** (able to process instructions from more than one program at the same time) and many servers have multiple network interface cards (NICs) or a much faster NIC, so that they have a better connection to the network.

Some of the many different types of servers include:

- file servers, which store files for use on client computers. They act as a central storehouse for shared files and for files that might be used in more than one computer at different times by the same user
- print servers, which accept print jobs over the network much faster than a printer could and then send the information to the printer when the printer is ready for it. The workstation is then able to get on with other tasks while printing takes place in the background
- database servers, which hold databases and allow them to be used by many users. Generally, when a user opens a record it cannot be opened by any other user until the current user closes it. The database files used in schools to store student information (e.g. CASES) would reside on a database server
- web servers, which are connected to the Internet and serve webpages to viewers upon request. A web server holds many files and pictures in a read-only format, so that many people can open copies of the files at any one time
- domain name servers (DNSs), which translate domain names into IP addresses. Browsers operating on the network request the DNS to provide the IP address so that it can then locate the required website or mail server. If it is an internal DNS, a list of the machines on the intranet and the number of the nodes to which they correspond is stored by the DNS
- proxy servers, which keep a copy of all recently accessed webpages and files so that if a page is requested again (and it has not been changed) it is delivered from the proxy rather than from somewhere out on the Internet
- backup servers, which act as fast backup machines for other machines on the network
- dynamic host configuration protocol (DHCP) servers, which hand out the node number to each device
- active directory domain controller, which is a server that is running Active Directory Domain Services (AD DS). An AD DS stores directory data and manages communication between users and domains, including user logon processes, authentication and directory searches.

All of these servers could be connected to a network and each would handle requests from the attached client workstations and send out data.

Smaller organisations run multiple servers on the one machine because not every type of server is being used all of the time. As networks grow bigger, it becomes more efficient to spread the workload across more machines.

You see multi-tasking every time your computer processes a print job 'in the background' while you continue to work.

Network Interface cards are discussed later in this chapter.

A growing trend in many organisations is to use a virtual server rather than a separate physical device for each server. Software is used to partition a single server so that it operates as several servers, each able to run its own operating system and reboot independently.

A domain name server converts domain names into IP addresses. When the DNS receives a request from a browser to provide an IP address, it can:

- answer the request if it already knows the address
- contact another name server and request the IP address. This may need to be repeated multiple times
- return an error message that announces that the address was invalid or could not be found.

A primary domain controller (PDC) server was part of the pre-Windows 2000 NT operating system and was replaced by active directory domain services (AD DS) in more recent versions of Windows (e.g. Windows Server 2008R2). The main difference is that an AD DS does not have primary and backup domain controllers. Instead, the domain controllers in these domains are all considered to be equal, and all controllers have full access to the accounts databases stored on their machines.

A 'peer' is someone on the same level as you. In a client-server model, the servers are regarded as superior because they have the right to share, whereas clients do not.

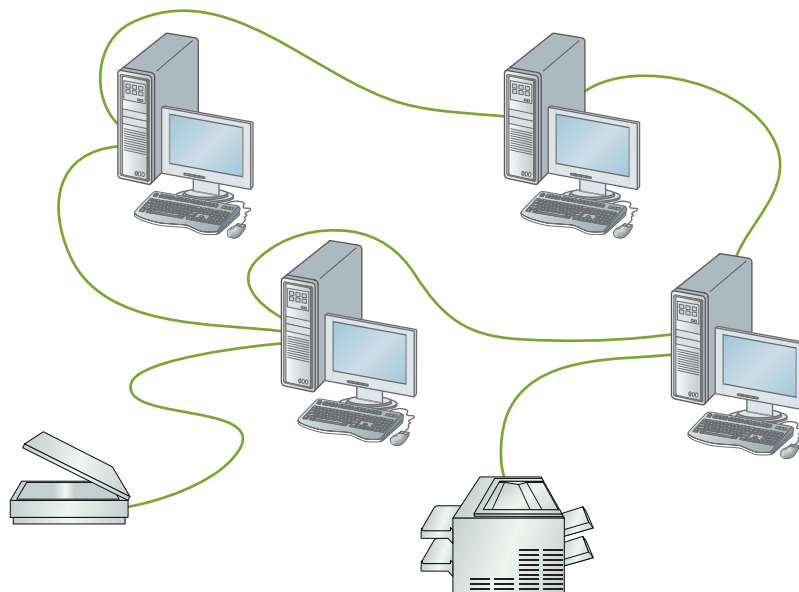
Peer-to-peer network

In a **peer-to-peer network**, all devices are able and allowed to share files and resources (Figure 1-7). The difficulty with the peer-to-peer scenario is locating which resource is available on which machine and then waiting for the machine to deliver that resource over the network. The operating system on a workstation is usually configured to give priority to the person at the keyboard, making others on the network wait for a suitable gap in usage. This limits the efficiency of the network, so they are mostly used when a small, inexpensive solution is needed, such as in a home network.

Each computer on a peer-to-peer network allows the files stored on it to be shared and will serve them out to other users. Depending on the individual configuration, this serving might have to be authenticated. The authentication process requires users to set up a folder on their hard drive from which only known 'peers' can access the shared files. To be known as a 'peer', the username has to be on an approved list contained in the computer being accessed.

Each computer on the network stores files on its own storage device and has both the network operating system and application software loaded. Peripheral devices such as printers and scanners are shared between all computers on the network.

In a simple home network with no outside connections, most people will run a peer-to-peer network so that they can store files on any machine and access them from any other machine. This ensures that they keep only one copy of their data (aside from the backups) to avoid confusion. It also means that any machine is available for use as a workstation. When the workstation is acting as a server – that is, actually serving out files – it is noticeably slower to respond to the user. This is because it is busy



Printer may be used by all computers on the network

FIGURE 1-7

Each computer on a peer-to-peer network shares its hardware and software with other computers on the network.

communicating with another computer. In a home situation, this does not really matter as there is only ever a small number of users and the inconvenience is minimal. In an organisational setting, however, it can have a profound effect as there are many more people wanting to access some files. The workstation does not have the internal configuration to easily serve out files and so it is slow to respond.

Internet peer-to-peer network

An **Internet peer-to-peer** network allows users to connect to someone else's computer over the Internet. Users are thus able to share files by copying directly from the hard disk of the other person's computer and saving the files to their own hard disk. Users must enable their computer to be used for file sharing and their computers must be logged onto the Internet at the time.

BitTorrent, LimeWire and Kazaa are popular software applications that support Internet peer-to-peer. These programs allow users to copy MP3 music and other media files from one computer to another.

Allowing Internet peer-to-peer file sharing exposes your computer to possible security violations. Malicious software (see later in this chapter) capable of causing computers to malfunction or seize can be transmitted via peer-to-peer networking. Recognised sites, such as LimeWire, often have built-in security measures, but how dependable these are is open to question and using such sites can be risky.

BitTorrent is an Internet peer-to-peer protocol for sharing very large media files. Transferring large files can put considerable strain on a computer, particularly a portable device with low bandwidth. Using BitTorrent, a user makes a media file available to the network. This first user's file is called a seed and its availability on the network allows other users, called peers, to connect and begin to download the seed file. As new peers connect to the network and request the same file, each computer receives a different piece of the data from the seed. Once multiple peers have multiple pieces of the seed, BitTorrent allows each to become a source for that portion of the file. The effect of this is to take on a small part of the task and relieve the initial user, distributing the file download task among the seed and many peers. The result is that all peers receive the complete file, but no single computer has had to supply a large file to multiple users, thus avoiding the overtaxing of the original source computer.

Issue

Digital music sales 'to nearly equal CDs next year'

Compact discs accounted for 65 percent of US music sales in the first half of 2009 but digital downloads are expected to nearly equal CD sales by the end of next year, said market research firm NPD Group.

'Many people are surprised that the CD is still the dominant music delivery format, given the attention to digital music and the shrinking retail footprint for physical products,' said Russ Crupnick, NPD vice president of entertainment industry analysis.

'But with digital music sales growing at 15 to 20 percent, and CDs falling by an equal proportion, digital music sales will nearly equal CD sales by the end of 2010.'

Paid digital music downloads accounted for 35 percent of all music sales in the first six months of the year, up from 20 percent in 2007 and 30 percent last year.

According to NPD, Apple's iTunes accounts for 25 percent of all music units sold, up from 14 percent in 2007 and 21 percent in 2008.

Walmart, the world's largest retailer, was next, accounting for 14 percent of music volume sold, followed by Best Buy.

'The growth of legal digital music downloads, and Apple's success in holding that market, has increased iTunes's overall strength in the retail music category,' said Crupnick. 'But the importance of the big box retailers shouldn't be dismissed, as long as the majority of music consumers continue to buy CDs.'

Think about IT 1-5

- 1 Will legal music download sites lead to the demise of Internet peer-to-peer sites such as LimeWire? Is this a good thing?
- 2 Why do you think music downloading is gaining popularity over CD sales?
- 3 Research the Internet to find out how Kazaa has reinvented itself to become a legal music sharing site.

Consumer downloads from iTunes comprised 69 percent of the digital music market in the first half of the year, NPD said, followed by AmazonMP3 at eight percent.

Walmart was the top-seller of CDs with a 20 percent share of the physical music market, followed by Best Buy at 16 percent and Target and Amazon at 10 percent each.

(Source: © 2010 AFP, *The Age*, 19 August 2009)

If the LAN in an organisation provides access to the Internet, the intranet must reside behind a firewall to protect it from access over the Internet.

Think about IT 1-6

List the information, documents and resources that are available on your school's intranet. Do teachers have permission to change any part of the intranet? What additional features would you expect to see on the intranet in five years' time?

A comprehensive listing of data communications protocols, including their function and structure, can be viewed at www.protocols.com.

The Institute of Electrical and Electronic Engineers (IEEE) sets standards for most types of electrical interfaces. For example, the RC-232c standard defines an interface for serial communication that is used by most modems. IEEE also developed the 802.11 standard for wireless communication.

Intranets

An **intranet** is an internal, secured environment that has a similar look and feel to the Internet, but operates as a local area network. An intranet provides easy and fast access to information by employees in a familiar environment while keeping the information secure from the general public.

The benefits of intranets include:

- access to information in a controlled manner
- communication within the organisation; for example, news, notices, organisational style sheets, maps of building locations, guidelines, policies and telephone numbers can be published on the intranet
- messages that log hardware and software problems with technical support personnel
- contacts of who to approach for various problems or issues
- bi-directional mechanisms; for example, online forms and document reviews
- training through the publication of online user guides and computer-based training programs.

Intranets can reduce costs within an organisation since they require less paper (documents available electronically), reduce the number of queries from employees, take less time to find data (especially if the intranet has a built-in search engine) and require less document maintenance (a single repository for important documents that can be easily updated).

Network communication standards

For different devices on a network to be able to communicate, they must use similar techniques for moving data through the network from one application or resource to another. **Network standards** have been established to overcome the problems of incompatibility on a network and to ensure that hardware and software components can be integrated into any network.

A network standard defines a set of guidelines that manufacturers must follow in the design and production of their hardware or software products. The guidelines specify how computers access the network to which they are attached, the type of medium used, the speed of data transfer across the network, and the types of cable or wireless connections that are supported. Without standards, only hardware and software from the same company could be used together.

A **protocol** is a standard that defines how two computers or devices on a network transmit data. The protocol determines:

- the type of error checking used
- the data compression method, if one is used
- how the sending device will indicate that it has finished sending a message
- how the receiving device will indicate that it has received a message.

From a network user's perspective, the important thing about standards and protocols is that your computer or device must support the right ones if you want to communicate with other computers.

Several widely used network standards and protocols are discussed in the following sections.

Ethernet

Ethernet is a network standard that describes communication over a single cable shared by all devices on the network. A device connected to the cable is able to communicate with any other attached device. This allows the network to expand if additional devices need to be connected without requiring any changes to those devices already on the network.

Ethernet communicates between nodes in short messages called **frames**, which contain packets of information. The frames are individually sent by the sending device and receipted back to the sender from the receiver. All of the frames contain the destination node address, the sending node address and some data. The address uniquely identifies the node. The frames also contain **parity** information, to check if the frame has arrived correctly (Figure 1-8).

Every computer or device recognises when data on the network is being sent to it because each frame of data has the address of the destination machine as the first part of the frame. Anything addressed to another computer is ignored – it is not accepted by the computer and so does not enter the device. The computer only has to be able to read the first part of the packet to know whether or not to accept the data. When a computer accepts a frame, it checks to ensure that the frame has arrived correctly. (The length and the parity of the packet are contained in the address part of the frame because if the address survives the trip, the checking information should as well.)

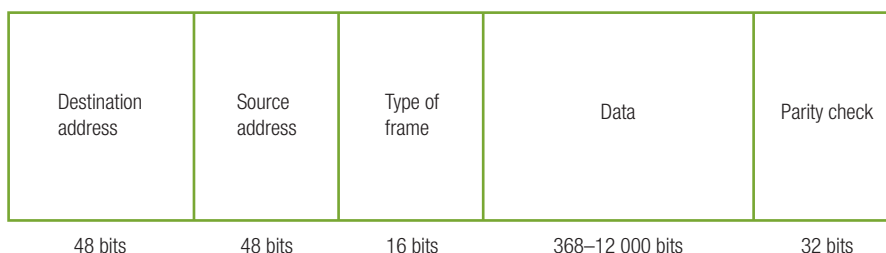


FIGURE 1-8

An ethernet frame contains the destination node address, the sending node address, data and parity check information.

The Open Systems Interconnection (OSI) is a standard for network communications that defines a model for using protocols in seven layers. Each layer only uses the functions of the layer below it, and only passes functionality to the layer above. A description of the OSI model can be found at http://en.wikipedia.org/wiki/OSI_model.

The first ethernet network was designed and tested in 1973 at Xerox Corporation's Palo Alto Research Centre by Bob Metcalfe.

Parity is where the data (in binary code data is represented by 1s and 0s) in the packet are added together as if they were numbers. If the result is an odd number, the parity bit is set to 1, and if the result is even it is set to 0. This is the same concept as the check digit on bar codes.

The network interface card inside a computer is the direct connection between the computer and the network and makes decisions whether to accept or ignore an ethernet frame.

The random delay is important after a collision. If two nodes are trying to transmit at the same time and a collision has occurred, they both will need to transmit again. If they both resent their messages at the next available quiet time, they would most likely collide again. The random delay ensures that it is unlikely that two messages will collide more than a few times in a row.

Ethernet was originally designed to operate on a LAN, usually within a single building. Ethernet networks originally could only be a few hundred metres long, making them incapable of connecting widely separated buildings. Advancements over time have allowed ethernet networks to expand their range considerably.

The TCP/IP protocol is not restricted to a single manufacturer, unlike many of the other available protocols, such as Apple File Protocol (AFP) from Apple Computers, Microsoft's NetBIOS Extended User Interface (NetBEUI), Novell's Sequential Packet Exchange (SPX) and Internetwork Packet Exchange (IPX).

NetBEUI is a network protocol used in DOS and Windows 3x computers. It can be used only on a single LAN segment and is not formally supported by Windows. IPX is a network protocol used in Novell's Netware operating system. SPX provides error recovery functions for data delivered by Netware's IPX protocol. IPX performs similar functions to the IP protocol in TCP/IP, while SPX performs similar functions to the TCP layer.

Packet switching is the term used to describe the process of breaking a message into several small packets, sending the packets along the best available route (individual packets may travel different routes) and then re-assembling the data at the destination.

When a frame is accepted, an acknowledgement is sent back to the originating computer indicating that the device is ready for more data. If the frame is faulty, a resend request is sent to the originating computer.

Since the ethernet standard does not use a central computer to control when data can be transmitted, a node must 'listen' to the network to determine if another computer is transmitting a frame. If the network is quiet, the node recognises that it is an appropriate time to transmit. If two or more computers judge that the network is quiet and each proceeds with a transmission, a collision occurs. When a node detects that a collision has occurred (their transmission is returned in a garbled form), it ceases further transmissions and waits a random amount of time. The node again checks to see whether the network is quiet before it resends the message.

The length of cable shared on an ethernet network must be short enough that devices at opposite ends are able to receive each other's transmissions clearly and with minimal delay. As the length of the cable increases, the electrical signals that carry the ethernet frames weaken. Interference from other electrical appliances can also affect the frame. These restrictions impose a limit to the length of an ethernet network.

Early ethernet transmissions were comparatively slow by today's standards. Figure 1-9 shows the data transfer rates of recently developed ethernet standards.

TCP/IP

The most common method of packaging data for network transmission these days is **TCP/IP** (Transmission Control Protocol/Internet Protocol). This is the protocol on which the Internet is based. The TCP/IP protocol defines how data is carried from one part of a network to another. The standard specifies the rules used to construct **packets** of data, the address scheme for the sending and receiving devices, an error-checking mechanism and how the flow of messages around the network is regulated.

TCP/IP uses a small packet size compared to other network protocols. This is a distinct advantage on the Internet. There are usually many different pathways from the originating device to the destination device and the packets do not necessarily all travel the same path. Smaller packets give many more options to the network management software to enable load balancing. Sequencing information sent with the packets is used by the receiving device to reassemble the data from all of the packets that it has been sent. In a LAN there is usually only one available path, so packet size is much less important.

The network standard for transmissions over the Internet is TCP/IP, so all hosts on the Internet must follow this standard. The use of TCP/IP enables a LAN network to easily support web servers, so the publishing of webpages internally on the network is not complicated. These same web servers can also simultaneously publish to the Internet.

802.11 wireless standard

The **802.11 standard** defines how two computers or devices can communicate using radio waves. A network that uses the 802.11 standard

Ethernet type	Cable type	Maximum length	Topology	Transfer rate
10BASE2 (thin ethernet)	Thin coaxial	180 m	Bus	10 Mbps
10BASE2 (thick ethernet)	Thick coaxial	500 m	Bus	10 Mbps
10BASE-T	Two twisted pairs (Cat 3 or Cat 5)	85 m	Star	10 Mbps
10BASE-FL	Fibre-optic	2 km	Star	10 Mbps
100BASE-TX (fast ethernet)	Two twisted pairs (Cat 5)	85 m	Star	100 Mbps
100BASE-FX	Multimode fibre-optic	2 km	Star	100 Mbps
	Single-mode fibre-optic	10 km	Star	100 Mbps
1000BASE-T (gigabit ethernet)	Two twisted pairs (Cat 5e or Cat 6)	85 m	Star	1 Gbps
1000BASE-SX	Multimode fibre-optic	220 m	Star	1 Gbps
1000BASE-LX	Multimode fibre-optic	550 m	Star	1 Gbps
	Single-mode fibre-optic	2 km	Star	1 Gbps
10GBASE-T	Two twisted pairs (Cat 5e, Cat 6 or Cat 7)	85 m	Star	10 Gbps

FIGURE 1-9

Ethernet transmission rates

is known as a **Wi-Fi** network. Wi-Fi networks allow computers that are up to 50 metres apart to be connected without the need for wires.

Wi-Fi networks that use the 802.11b or 802.11g standards transmit data at a frequency of 2.4 GHz, while the 802.11a standard uses 5 GHz. The newer 802.11n standard operates at 5 GHz or 2.4 GHz and is expected to be faster and support a larger range (up to 70 metres indoors) than previous standards. The higher the frequency, the higher the data transfer rate. Figure 1-10 compares the frequencies used and data transfer rates for the 802.11 series of standards.

Computers fitted with a 802.11 wireless network card can split the available radio bandwidth into a number of channels and frequency-hop rapidly between them. Frequency hopping allows a number of computers using wireless cards to talk simultaneously without interfering with each other.

Most new notebook computers come with a Wi-Fi network card already installed. Often, the antenna required to transmit signals via radio waves is

10BASE-T is an acronym for 10 Mbps, baseband, twisted-pair. Baseband refers to the transmission of digital pulses (bits of data) without any additional modulation. A broadband signal is frequency modulated. All digital processing is baseband, so LANs operate using baseband signals. The full bandwidth of the channel can be used to transmit bits of data.

Multimode fibre-optic cable uses multiple light pulses set at different angles to transmit data. Light signals dissipate over long distances, so multimode cable is only used for shorter connections. For longer connections, single-mode optic-fibre cable is used. Single-mode cable and the equipment needed to make connections are usually more expensive than multimode cable.

VCAA will not expect students to recall the data in this table. It is provided for interest only.

Wi-Fi stands for wireless fidelity.

The 802.11 standard comes in different versions signified by an a, b, g or n notation. The first version to reach consumers was the 802.11b standard, followed more recently by 802.11a, 802.11g and 802.11n standards.

The 802.11n standard was ratified at the end of 2009. The standard can operate at either the 2.4 GHz or 5.0 GHz frequencies. The 5.0 GHz frequency is used if there is any possibility of interference from another device, such as another network using a 802.11 standard, or a non-802.11 device such as a microwave oven or a Bluetooth device (which operate on the 2.4 GHz frequency).

Standard	Radio frequency	Transfer rate
802.11a	5.0 GHz	Up to 54 Mbps
802.11b	2.4 GHz	Up to 11 Mbps
802.11g	2.4 GHz	54 Mbps and higher
802.11n	5.0 GHz or 2.4 GHz	108 Mbps to possibly 600 Mbps

FIGURE 1-10

Comparison of frequencies and data transfer rates for the 802.11 series of standards

built in around the screen of the notebook. Older desktop computers need to have a wireless card installed.

The 802.11 standard uses techniques that are similar to the ethernet standard to control data flow. For this reason, a Wi-Fi network can be easily connected to a wired ethernet network.

Network hardware and software

We have considered in previous sections the various types of networks that an organisation might use and the communications standards that govern how devices on the network are able to talk to each other. A network also requires a number of hardware and software components to allow computers to communicate with each other. In this section, we will look at several common network components.

Network operating systems

The **network operating system** is software that controls traffic on the network and defines how devices will communicate with each other. A network operating system usually has two components – server software and client software.

Network server software is installed on the network servers and performs tasks such as controlling file access, managing print queues, keeping track of users through their UserIDs and passwords, authenticating access to network servers and maintaining a log of network usage and problems (Figure 1-11).

Network client software is installed on each workstation and establishes a connection, through the network interface card, between the workstation and other devices on the network. Individual workstations use the network operating system to create their own data packets and transmit them at appropriate times to ensure successful communication.

There are three significant providers of network operating systems used with personal computers – Microsoft Windows Vista, Windows 7 and Windows Server 2008; Novell and Apple. Microsoft is now the dominant system and both of the other systems have designed their code so that clients running Novell or Apple can also recognise servers from the other two systems. This has meant that users can run a particular network operating system and still access machines on other networks. This can

Network operating systems have existed for more than 30 years. In its early form, however, Windows did not support networking, so Novell Netware became the first popular network operating system for personal computers. Most operating systems available today qualify as a network operating system due to the popularity of the Internet and the need to conform with Internet Protocol (IP) networking.



FIGURE 1-11

Network server software controls file access, manages print queues, maintains usernames and passwords, and authenticates access to servers.

be very helpful in situations where companies have merged, or in schools where there are a number of separate networks that need to be connected. It is preferable for all machines on the same network to be using the same network operating system, as it makes network maintenance simpler. It also ensures that, as there is only one set of instructions for the users, they can help each other where possible.

Web client software

Web client software includes web browsers, electronic mail, videoconferencing and instant messaging.

A **web browser** allows a user to view pages on the Internet and manages the links used to jump from one document to the next. Today's web browsers have replaced a number of separate Internet client software programs that used to be required to access different types of Internet servers. For example, FTP, Archie, WAIS, TelNet and Gopher client software are now included in most browsers. A web browser can now be used to view webpages, transfer files between computers, send email and to interact with other Internet users.

Common web browsers are Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Apple Safari and Opera.

Electronic mail (email) applications operate over a network such as the Internet or an intranet. Simple text messages can be sent to other users of the network. Email also supports the ability to attach a file for transmission with the message. Electronic mail software is included with most software suites. A network will usually have a mail server that is used to manage the flow of electronic mail. Incoming mail from other mail servers on the Internet is received and directed through the network to the recipient. Outgoing mail is directed by the mail server to its destination.

In December 2009, the usage share of web browsers was claimed by Wikipedia to be Internet Explorer 62.7%, Mozilla Firefox 24.6%, Google Chrome 5.0%, Safari 4.6%, Opera 1.3% and other 1.8%.

**FIGURE 1-12**

Videoconferencing brings people together electronically.

Videoconferencing software allows the transmission of audio and video signals over the Internet. Videoconferencing is used to bring people together electronically for a meeting (Figure 1-12). A video camera, microphone and speakers must be connected to users' computers.

Instant messaging involves the real-time exchange of messages and files between online users of a network.

A **chat room** involves users of the Internet engaging in real-time typed 'conversations'. Some websites provide chat rooms where a number of people can simultaneously take part in a conversation. As one participant types a message, it will appear on the screen of all the other people involved in the chat.

Different ports are used for different services provided by servers. For example, connection to a web server for Internet pages is via port 80, while port 21 is used for FTP and port 25 for email. You could set up a server and specify a different port for webpages, but the URL used by the client's browsers would have to specify the port to be used. When the default port of 80 is used, the port number does not need to be included in the URL.

The most basic form of the http protocol understood by a web server is the GET command. A server that obeys the http protocol that receives a GET command followed by a filename will serve that file to the requesting browser and then disconnect. If no filename is specified, the default or index page is sent.

Software for setting up websites

When a user requests a webpage be sent to their computer, they enter the page's **uniform resource location (URL)** into the web browser on their computer. The web browser uses the URL to request the required page from the host web server. The URL sent by the requesting browser includes the protocol to be used for the communication, the name of the server hosting the page, and the name of the page being requested. For example, if you were requesting to view a page on the Cengage resources site, you would enter the URL <http://cengage.com.au/ITApplications/resource.htm> into your browser. The first part of the URL is the protocol (http), followed by the name of the host web server (cengage.com.au) and then the name of the file you wish to load (ITApplications/resource.htm).

Hypertext transfer protocol (http) is a standard used for transmitting and receiving information on the Internet. All servers and computers on the Internet must follow the request and response procedure established in the http protocol so that information flows easily and quickly between servers and clients. The http protocol is used to access pages written in hypertext markup language (html).

The browser communicates with a domain name server (DNS) to translate the server name (cengage.com.au) into an IP address. (We discussed the TCP/IP standard earlier in this chapter.) Using the http protocol, the browser sends a 'get' request to the IP address of the web server for the required resource or page.

The server then serves the page in html code to the browser. The browser uses the html tags to format the page for viewing on the user's screen.

Website software

To set up a website for use on a network you need to have a web server running web server software, as well as a number of web software applications that sit on top of the web server software.

Web server software provides content using the http protocol. The content is usually in the form of html documents, images or other resources. There are many examples of web server software. Popular ones include Apache and Microsoft Internet Information Services (IIS).

When the web server software receives a 'get' request from a client's browser, it appends the path of the resource given in the URL to the path of the web server's root directory. The web server will then follow the path and if the resource exists it will then send that resource to the requesting browser.

To transfer a page to a client's browser, the web server needs to know the client's IP address. This means that the client is not anonymous to the web server. A **proxy server** can be used to sit between the client and the rest of the Internet. When a client's browser requests a page be loaded, the request can go to a proxy server that substitutes its IP address for that of the client. The website that receives the request is not able to identify the user. When the proxy server receives the page from the website it is then able to direct that page to the user.

Another use for a proxy server is to speed up network traffic by caching pages. If a client requests a page from a website that has previously been sent to the proxy server, the proxy server uses the page or file in its cache rather than reconnecting with the website. This means there is less demand on the server and the client receives the page faster than if a connection to the originating website was required. This is particularly useful in sites, such as schools, where the same webpages may be requested a number of times by different users.

Proxy servers can also be configured by network managers to block certain websites.

Simple mail transfer protocol (SMTP) is used on electronic mail servers to handle the sending and receiving of client emails. Small organisations may elect to combine several server applications on the one device, so the SMTP server may reside on the web server, but use different ports.

When a client sends an email, their email application, such as Outlook Express, connects to port 25 on the SMTP server on their host network. The SMTP server is given the address of the sender, as well as the address of the recipient and the text to be sent. The server separates the recipient details into their name and the domain name at which the recipient

Microsoft packages IIS with their Windows Server 2008 software.

In 1989, Tim Berners-Lee proposed a system to help scientists at the European Organisation for Nuclear Research (CERN) in Switzerland to exchange information. His system used hypertext transfer protocol and he developed two programs: the first was a browser titled WorldWideWeb, and the second was a web server called CERN httpd.



FIGURE 1-13

In 1989, Tim Berners-Lee proposed a hypertext system to allow scientists to easily exchange information. This was the birth of the World Wide Web.

accesses their email. The server then consults with a domain name server to establish the IP address of the recipient's mail server. The client's SMTP server then connects to the recipient's SMTP server and transfers the message.

A **Post Office Protocol (POP3)** server is used to store messages. When the SMTP server receives an email for a user on its network, either from another client on its network or from an external SMTP server, it passes the message to the local POP3 server, where it is stored until the client is ready.

File transfer protocol (FTP) software enables the uploading and downloading of files between computers on the Internet. FTP software is located on a server, possibly the same device as the SMTP and POP3 server, and uses port 20 for data transfers and port 21 as a control port. FTP uses TCP/IP protocols to enable file transfers.

Web software applications are programs designed for use on a website and include blogging software, forums and wikis. As discussed earlier in this chapter, software applications to enable blogs (for example WordPress) and forums (for example phpBB) work in collaboration with web server software.

Cross-platform web software

Generally, software applications are written to comply with the specifications of a particular operating system and hardware architecture. The operating system and hardware architecture that a computer uses is called its platform. Software applications must be compatible with the computer's platform. Rather than depending on the microprocessor and operating system of the computer, a **cross-platform** application uses an execution engine and compiler with libraries so that it runs identically on all machines. Examples of cross-platform software applications used in creating websites are Flash and Java.

Adobe Flash is a software tool that enables website developers to combine interactive content with text, three-dimensional graphics, audio and video (Figure 1-14). Animation and interactive tools, as well as high quality video capabilities, are popular features of Flash that developers embed in their webpages. These features can be implemented by all browsers and across all computer platforms.

Java is computer programming technology that allows website developers to create programs that will run within a web browser and other web services. Programs written using Java technology will run on virtually any platform. Online forums, polls and html form processing are all possible using Java technology.

Network interface card

A **network interface card (NIC)** is used to link a computer or resource to a network. The NIC is connected to the network by wires, radio waves, infra-red light waves, microwave or fibre-optic cable. These examples of transmission media are discussed later in the chapter.

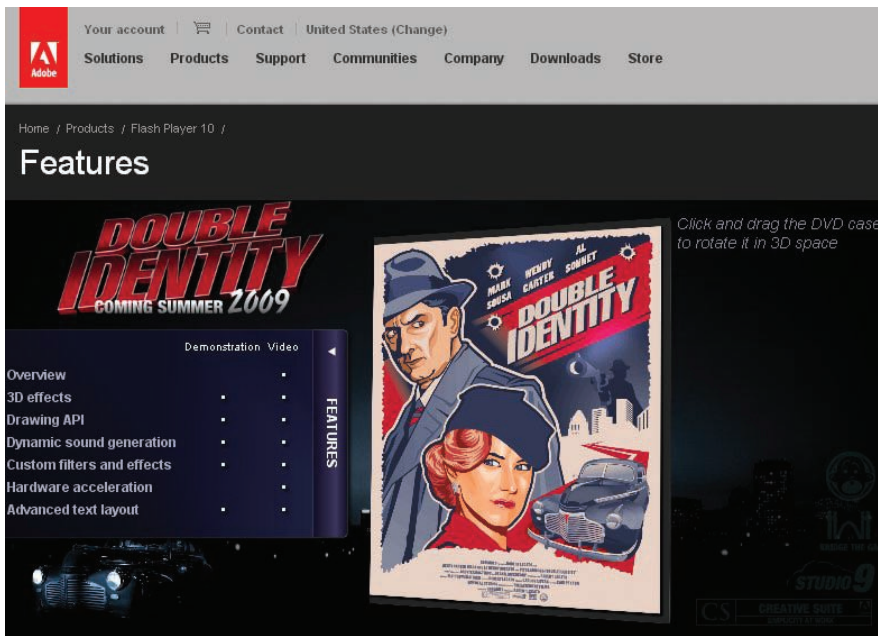


FIGURE 1-14

Adobe Flash allows web developers to create intuitive and engaging interfaces using 3D effects.

There are many different devices that can connect directly to a network through an NIC. The most important of these include computers, servers, printers, scanners, photocopiers, faxes and routers. Each network interface is called a node and is assigned a unique number within the network.

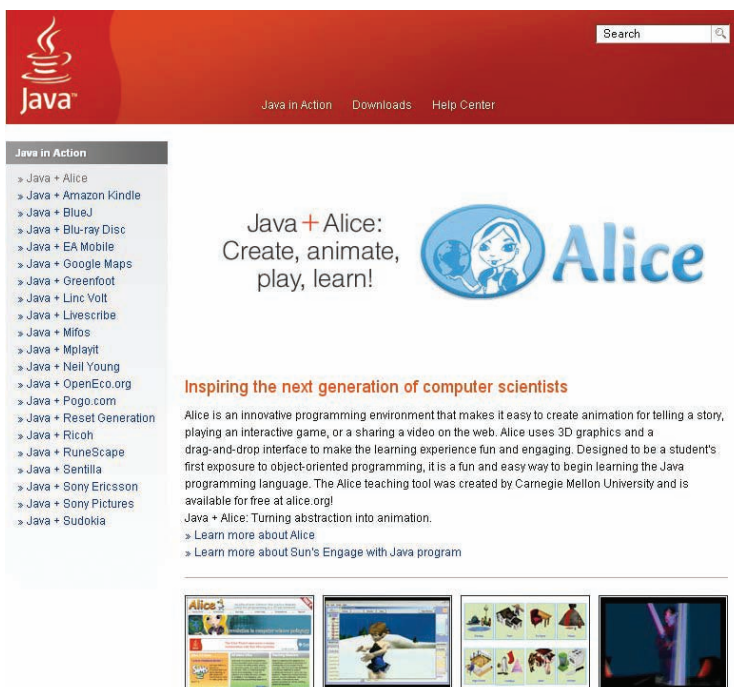


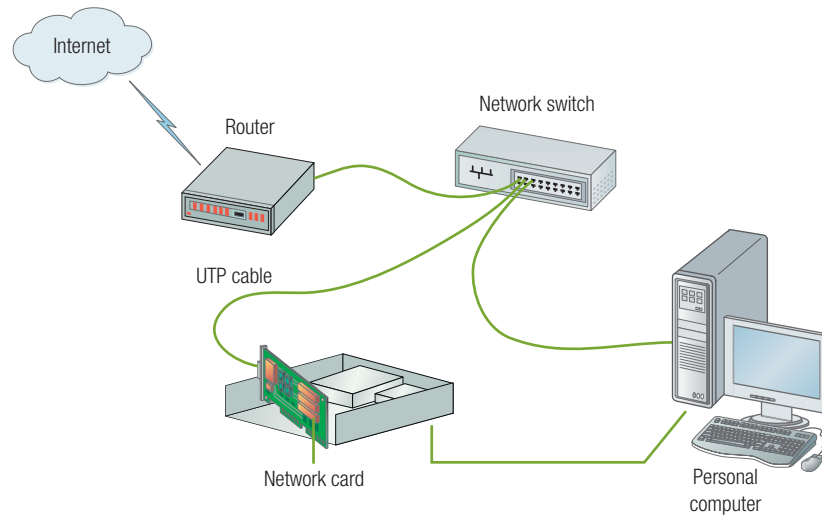
FIGURE 1-15

Java allows a website developer to create programs that run within a web browser.

Consider how many devices are connected to the Internet. Every one of them has a unique number within the entire Internet. The highest number on the Internet is 255.255.255.255. This gives 256 times 256 times 256 times 256 possible numbers for different nodes. Over 4000 million nodes can be present on the Internet – 4 294 967 296 actually!

The number 255 was used because it is 2 to the power of 8 less one, so can be represented by 1 byte in binary code (8 bits).

Also, we multiplied by 256 because the digit 0 (zero) is a valid position. The node number 127.0.0.1 is generally used to refer to your own computer.

**FIGURE 1-16**

A network interface card connects a computer workstation to a network.

The network interface card coordinates the transmission and receipt of data, instructions and information to and from the computer containing the network card (Figure 1-16).

Wireless access point

A **wireless access point** (AP) is used to connect wireless communications devices to a wired or wireless network. Often, an AP is connected to a wired ethernet network, which allows it to relay data between devices on each side of the AP (wired network on one side and wireless devices on the other). Where a number of APs are connected to a wired network, users are able to move from one area to another and maintain their network connection. The connection transfers to a different AP when the user moves out of range of the initial AP. This process of being able to move around a network is called **roaming**.

A wireless client connected to a wired ethernet network via an AP has full network access to all devices and servers, with the benefit of mobility.

A **hot spot** is a location where a user with a wireless-enabled computer is able to communicate with an AP. Many organisations, such as cafés,

Think about IT 1-7

- 1 Local broadband suppliers in Swindon may not be happy with the borough-wide Wi-Fi proposal, fearing that it will take business away from them. Are their fears warranted?
- 2 Do you see an issue with the local council having some control of the content and access to information through the Wi-Fi network?

Issue

Swindon promises city-wide Wi-Fi

Swindon in the UK is planning a borough-wide Wi-Fi network providing free Internet access to all residents. Swindon Borough Council has a 35 percent stake in the proposed public-private partnership to set up a provider named Digital City UK. Residents in the borough are expected to be able to access the Internet for free. The council and its partners will be able to use the technology to provide cutting edge services to the areas or individuals who need them. Residents will be able to 'seamlessly'

move between access points with no interruption to service. The council suggests the network could be used not only for free web access, but also for air-quality monitoring, free voice calls, wireless CCTV coverage, smart metering communications and telemedicine applications. Digital City UK's business model is built around subsidising free access with revenues from business and community services that are delivered over the wireless network.

The network will be launched with speeds of up to 20 Mbps, with faster services available to residents prepared to pay. Wireless repeaters will be supplied for installation in windows, so signals can be improved indoors. The free access is based on a limited time rather than a limited speed. Users would be able to gain free access at the maximum available speed for two hours a day, which is expected to be sufficient for basic needs. The network will be protected with the WPA encryption standard and no devices connected to the network will be accessible from the outside world.

(Source: David Meyer, ZDNet UK, 17 November 2009, <http://news.zdnet.co.uk/communications/0,1000000085,39884653,00.htm>)

hotels and airports, provide hot spots for the benefit of their customers. Customers with portable computers and wireless capability or smart phones are able to connect to the Internet without regard for the particular network to which they are attached at that moment (Figure 1-17).



FIGURE 1-17

Many businesses, such as cafés, now provide wireless hot spots to sell casual Internet access to customers.

Switches

A **switch** is a device that stores the address of every device down each wire leading from the switch. When a device talks to a switch, the first packet is examined for the destination device's media controller access (**MAC**)

The **MAC** address is a 48 bit hardware address that uniquely identifies each node of a network. Most networking equipment has a MAC address assigned to it.

The ability to transmit and receive data at the same time is referred to as a full duplex channel. The term 'duplex' means two-way. A half duplex channel is able to carry information in both directions, but not at the same time.

Internally, every computer has a bus system, which might operate at 132 MHz – so that it transports 132 Mbps along each wire. Most internal buses in a workstation consist of 64 wires for data, so the bus is really carrying 64×132 Mbps (= 8448 Mbps). The network, at its very best, can only carry 100 Mbps. A server often has an internal bus of 128 wires in parallel, and so can carry twice as much data around internally as can a workstation (= 16 896 Mbps), which is nearly 170 times more than the network can transport. This is why some servers use a fibre-optic cable running at one gigabit per second (1024 Mbps) to connect to the network.

- 1 gigabit (Gbit) = 1024 megabits
- 1 megabit (Mbit) = 1024 kilobits
- 1 kilobit (kbit) = 1024 bits
- A bit is either a one or a zero.

A **router** acts as a junction between two networks. It uses a routing table that stores the best route to certain network destinations.

address. Once the address has been found, it is matched with the switch's map of MAC addresses and corresponding switch ports. The packet is then switched to the appropriate port and sent down the wire containing the destination device.

The switching process allows simultaneous communication between different devices – workstation A can be requesting files from server B at the same time that notebook C is talking to workstation D. The switch acts as if the two devices are directly connected, and so they can send data at 100 Mbps uninterrupted. An ordinary switch can directly connect up to 40 pairs of devices in this fashion. In addition, switched devices can transmit and receive data at the same time, providing higher-performance networking.

In a peer-to-peer network, the use of a switch could be a big advantage if its capabilities could be fully used; however, they rarely are. The time taken to find the relevant computer, locate the material on it and wait for the local user of the computer to pause negates the benefit gained by adding a switch.

In a client–server network, the use of switches is unwarranted if there are only one or two servers on the network. Switches are very effective on a network that has a number of servers, so they are usually found in larger networks. A medium to large school typically uses switches to connect a print server, a web or intranet server, a proxy server (for Internet connection), a student file server (for home drives/personal areas), an administration file server and a library catalogue server on the network.

Routers

A **router** is a communications device that allows several remote LANs to connect over a WAN, or to join a number of LANs into one bigger LAN. A user on one LAN can access resources on another LAN through a router as if they were on the local LAN.

A router uses information contained within each packet of data it receives to route the packet to the appropriate LAN. Routers communicate with each other to provide information that allows them to determine the most efficient route to send a packet through a complex network of several LANs.

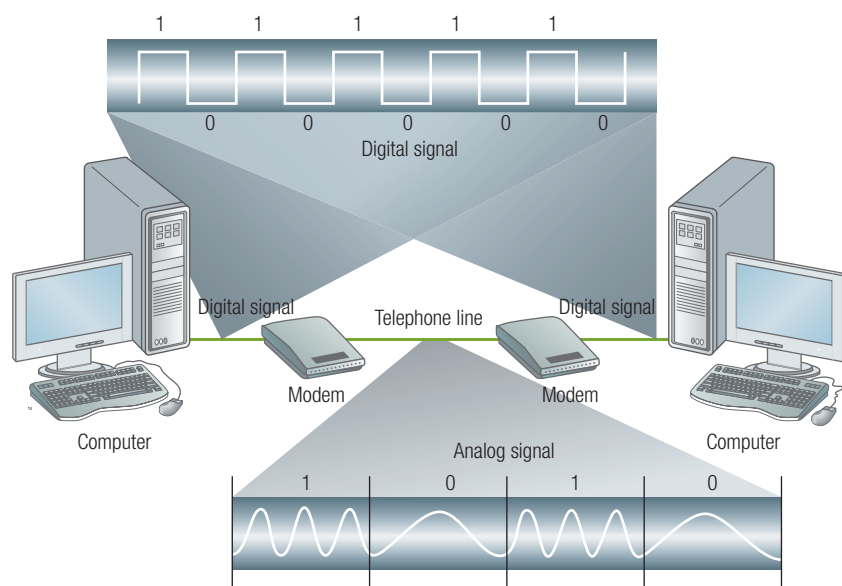
Modems

A **modem** is a device that is used to send a computer's digital signal over a telephone line. A sending modem modulates the digital data it receives from a computer into an analog signal that is compatible with the telephone line. A receiving modem demodulates the analog signal received from the telephone line into a digital signal that can then be transmitted to the receiving computer (Figure 1-18).

A dial-up modem is used with a standard telephone line. An integrated services digital network (ISDN) modem, an asymmetric digital subscriber line (ADSL) modem or a cable modem can be used, depending on the type of communications carrier used.

Dial-up modems

An external modem is a stand-alone (separate) device that attaches to a special serial port, such as RS-232, on a computer with a standard

**FIGURE 1-18**

A modem converts individual electrical pulses of a digital signal into analog signals for data transmission over some telephone lines. At the receiving computer, another modem converts the analog signals back into digital signals that the computer can process.

telephone cord connected to a telephone outlet. You can easily move an external modem from one computer to another.

An internal modem is a card that you insert into an expansion slot on a computer's motherboard. One end of a standard telephone cord attaches to a port on the modem and the other end plugs into a telephone outlet. Devices other than computers also use internal modems. A stand-alone fax machine, for example, has an internal modem that converts a scanned digitised image into an analog signal that can be sent to the recipient's fax machine. One advantage of internal modems over external modems is that they do not require desk space.

A notebook and other mobile computers can use a modem in the form of a PC card that is inserted into a PC card slot in the computer. The PC card modem attaches to a telephone outlet via a standard telephone cord. Mobile users without access to a telephone outlet can also use a special cable to attach the PC card modem to a mobile telephone, thus enabling them to transmit data over a mobile telephone. Most mobile users have a wireless modem that allows access to the Internet wirelessly from notebook and handheld computers, smart phones and other mobile devices. These wireless modems typically use the same radio waves used by mobile phones.

Digital modems

If you access the Internet using an **ADSL** connection, you need a communications device to send and receive the digital ADSL signals. A modem used for dial-up access will not work because it converts analog signals to digital signals and vice versa. In the case of ADSL, this conversion is not necessary. Both the computer and the ADSL connection already use digital signals.

A digital subscriber line (DSL) is a digital line alternative for the small business or home user. DSL transmits at fast speeds on existing standard copper telephone wiring. Some of the DSL installations can provide a dial tone, so you can use the line for both voice and data.

An asymmetric digital subscriber line (**ADSL**) is one of the more popular types of DSLs. ADSL is a type of DSL that supports faster transfer rates when receiving data (the downstream rate) than when sending data (the upstream rate). ADSL is ideal for Internet access because most users download more information from the Internet than they upload.

A 500 MB film or TV show can be downloaded in a little as:

Connection	Time to download 500 MB	Transfer speed
Dial up	19 hours and 38 minutes	56 kbps
ADSL	8 minutes and 20 seconds	8 Mbps
ADSL 2+	3 minutes and 20 seconds	20 Mbps
Broadband cable	2 minutes and 14 seconds	30 Mbps

A **digital modem** is one that sends and receives data and information to and from a digital connection such as ADSL or broadband cable. According to the definition of a modem (to convert from analog to digital signals and vice versa), the use of the term 'modem' in this context is not correct. Industry manufacturers, however, refer to ADSL modems as digital modems.

Cable modems

A cable modem is a modem that sends and receives data over the cable television network. Cable modems provide a faster Internet access alternative to dial-up for the home user. Cable modems can currently transmit data at speeds much faster than either a dial-up modem or ADSL (Figure 1-19). Today, many home and business users are taking advantage of the resources available on the Internet and other networks with high-speed cable service.

Telstra Internet plans Feb 2010	Transfer speed		Monthly fee	Usage
	Download	Upload		
Dial up	56 kbps	56 kbps	\$21.95	unlimited
ADSL Turbo	1.5 Mbps	256 kbps	\$79.95	25 GB
ADSL Elite	8 Mbps	384 kbps	\$89.95	25 GB
ADSL Elite	20 Mbps	1 Mbps	\$89.95	25 GB
Cable Elite	30 Mbps	1 Mbps	\$89.95	25 GB
Satellite	512 kbps	128 kbps	\$249.95	2 GB

FIGURE 1-19

Transfer rates and monthly fee comparison for Internet connection plans available through Telstra BigPond in February, 2010

Transmission media

Computers and devices on a network require some form of communications link to allow electronic signals to pass between them. A network communications link can use physical transmission media, such as twisted-pair, coaxial cable or fibre-optic cable, or wireless transmission media, such as radio waves, microwaves, satellite communications or infra-red waves.

Physical transmission

Early networks were always connected by wires or cables. Wired networks remain the most common type used by organisations. Cables are used within buildings and underground to connect remote buildings. Ethernet LANs typically use physical transmission media.

Twisted-pair cable

Most star networks use an **unshielded twisted-pair (UTP) cable** in which there are eight wires twisted in four separate pairs, and then

twisted as a group (Figure 1-20). The twisting helps to prevent outside interference because the wires are not running parallel to any outside cables.

CAT 3 cable can carry 10 Mbps reliably over 100 metres. CAT 5 cable has many more twists per metre and can reliably carry 100 Mbps over distances up to 85 metres. Only two of the wire pairs are actually used in CAT 5 cables. Two of the wires carry the signal to the switch and the two other wires carry signals from the switch. This immediately makes the network more efficient because messages from the NIC do not interfere with messages to the card.

CAT 5e (category 5 enhanced) cable uses all four wire pairs and can support 1 GB transmissions over short distances. Many star networks use CAT 5 or 5e cable while running at CAT 5 standards. CAT 6 cabling has more stringent specifications regarding noise and offers super-fast broadband. It is currently the most popular cabling for new installations. CAT 7 cable includes individual shielding of each of the four standard wire pairs and the cable as a whole, which allows 10 Gbps transfer. CAT 7 cabling is used for applications such as full motion video.

Coaxial cable

Coaxial cable contains only two wires (Figure 1-21). The inner wire is surrounded by insulation, and then by copper braid or sometimes aluminium, tin or lead foil, and finally another layer of protective insulation. The braid or foil is effective at shielding internal signals from outside interference. It is commonly used to connect a TV to the aerial.

Coaxial cable can reliably carry data over approximately 185 metres at 10 Mbps. It is used in bus networks, where all data travels in both directions away from any computer that originates a message. The cable carries the signal in both directions, so both incoming and outgoing messages from each computer are carried on the same wires. Thus when a device wants to send a message over the network it has to wait a lot longer for a gap in network traffic. This type of cable is typically used in situations where there are no switches, so all of the network traffic travels along all of the cable. Thus a single broken wire totally disrupts the network.

Fibre-optic cable

Fibre-optic cable consists of special glass or plastic strands that can transmit light pulses (Figure 1-22). The light is not susceptible to electromagnetic interference and so can reliably carry data for distances of up to two kilometres.

The speed of the data relies entirely on the quality of the light generator and the light receiver on the ends of the strand. The same strand can simultaneously carry pulses of light of different frequencies. This allows multiple users to make use of a single strand at exactly the same time. Currently, over 1000 different frequencies can be transmitted along a strand at the one time. The equipment to do this (a multiplexor) is still very expensive, but it is being used in areas where it is difficult to increase the number of strands available; for example, the undersea cable between Asia and Australia.

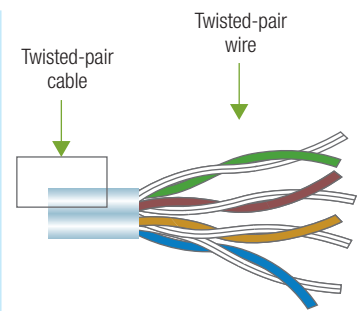


FIGURE 1-20
Unshielded twisted-pair cable

CAT 3, CAT 5, CAT 5e, Cat 6 and CAT 7 are the terms used to describe the UTP cable. Each type of cable is rated differently and so has a different name.

The specifications for CAT 5 cable are set by the EIA-568-B Commercial Building Telecommunications Wiring Standard. The standard specifies that the maximum distance for CAT 5 operation is 100 metres, though, in practice, network designers usually do not go above 85 metres for a network backbone and 5 metres for connection between a backbone and a network device.

Short coaxial cables are commonly used to connect home video equipment. They were also common for implementing computer networks, in particular ethernet, but twisted-pair cables have replaced them in most applications. Long-distance coaxial cable is used to connect radio networks and television networks, though this has largely been superseded by other more high-tech methods (fibre-optic cable and satellites).

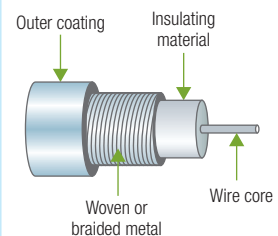


FIGURE 1-21
A coaxial cable

The light stays within the strand because of the physics phenomenon of total internal reflection. This means that the light reflects (bounces) off the inside wall of the strand and continues along the cable. If the cable is bent, severe light leakage can occur, so fibre-optic cable is usually encased in a thick plastic sheath and only bent gently at corners.

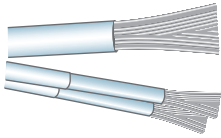


FIGURE 1-22
Fibre-optic cable

PIPE International has laid the PPC-1 undersea cable that runs 6900 km from Guam to Sydney. The cable will allow onward connection to Asia and the United States. The cable was configured as a two optic-fibre pair system, but will include an additional four optic-fibre pairs that will provide the potential to install additional spurs extending to a number of locations within and outside Australia. It will use multiplexing and was originally specified to provide up to 96 by 10 Gbps wavelengths on each fibre, producing a total of 1.92 terabits of capacity. This estimate was updated in December 2009 to 2.56 terabits per second.

Source: http://www.equinix.com/news/press/PIPE_International_Chooses_Equinix_en/

Microwave ovens also operate at 2.45 GHz. A Bluetooth device operating near a microwave oven is likely to experience some interference.

Fibre-optic cable is often used at just 100 Mbps because switches of that speed are relatively cheap. In many graphic design studios, gigabit speeds are needed because of the large files that are moved between machines.

Fibre-optic strands are only capable of handling one-way traffic. This is called simplex transmission. The transmitter is at one end and the receiver is at the other. Where two-way traffic is desired using fibre-optic cable (which is almost always), two separate strands are used. Thus two strands are used to achieve the equivalent of two-way transmission.

Wireless transmission

Wireless transmission is used where it is difficult to install cables or inconvenient to be tethered to the same spot. Wireless transmission includes the use of radio waves, microwaves, satellite and infra-red waves.

Radio waves

Radio waves can be transmitted over long distances, such as between cities, or over short distances, such as within a building. For radio transmissions to occur, a transmitter is needed to broadcast the radio signal and a receiver is needed to accept it. Radio transmission is more likely to be a victim of noise than a cable, but offers greater flexibility through its portability.

Wi-Fi networks, as discussed earlier in this chapter, use radio waves to transmit signals. Wireless network connections for notebook computers mean that they can be used anywhere within the range of an access point that will then connect them by cable (or a separate transmission) to the network. Wireless communications are slower than most cable connections, so it would not make sense to replace existing cable within a school or business with wireless transmission. Adding access points and Wi-Fi networking to existing wired networks, however, provides opportunities for users to connect with portable notebook computers or where adding more cable is not possible. For computer installations in heritage-listed buildings, wireless transmission becomes feasible so that no computer cables are in evidence in the rooms.

Bluetooth is a standard that uses short-range radio waves to transmit data over a distance of up to 10 metres. Data transfer is only at a rate of

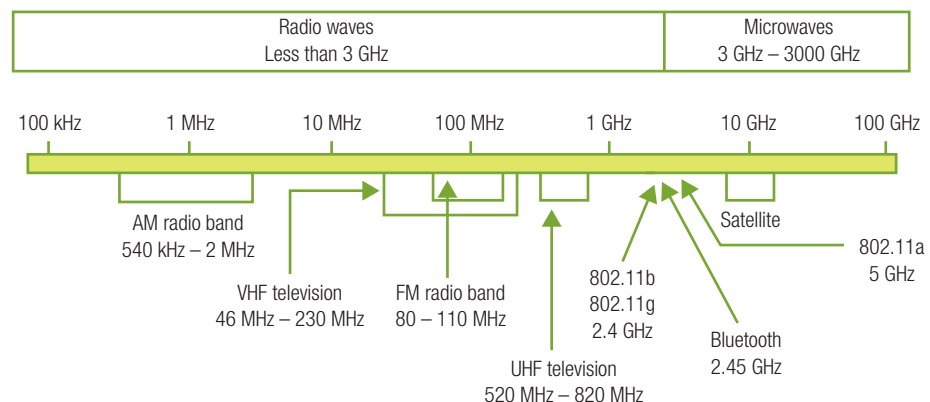


FIGURE 1-23
Australian radio frequency allocations

2 Mbps, compared to Wi-Fi transmission of up to 108 Mbps or higher over 100 metres. Bluetooth is useful to connect notebook computers in a meeting or to use in conjunction with hand-held computers, PDAs and smart phones. Bluetooth devices operate at a frequency of 2.45 GHz.

Microwaves

Microwaves require line-of-sight transmission where there is no obstruction between the sending dish and the receiving dish. Microwave transmission can handle very high data rates over short distances (e.g. 4 Mbps over 5 kilometres). The microwave spectrum ranges from 3 GHz to 3000 GHz.

Microwaves pass through the Earth's atmosphere with less interference than longer wavelength (smaller frequency) radio waves, such as the AM and FM radio bands. There is also more usable bandwidth in the microwave spectrum than in the rest of the radio spectrum.

A microwave station contains a concave dish that includes the antenna, transceivers and other equipment required for microwave transmission. Microwave stations are usually located on towers at the top of hills or mountains or on top of large buildings (Figure 1-24).



FIGURE 1-24

A microwave station located on a tower

Satellite

Satellite transmission can be in the form of radio waves or microwaves. The biggest limitation to this form of transmission is the distance the waves have to travel to the satellite and back to the Earth station. An Earth station transmits a signal to a satellite, which then amplifies the signal before broadcasting it back over a wide area to a large number of Earth-based stations.

Satellite communication is often used for television broadcasts, videoconferencing, global positioning systems (GPS) and Internet

The absorption by the Earth's atmosphere of electromagnetic radiation of frequency greater than 300 GHz is so great that the atmosphere is effectively opaque to higher frequencies of electromagnetic radiation, until the atmosphere becomes transparent again in the so called infra-red and optical window frequency ranges. Microwave transmission is therefore limited to a range 3 GHz to 300 GHz.

A satellite is a specialised wireless receiver–transmitter that is launched by a rocket and placed in orbit around the Earth. There are thousands of satellites currently in operation. They are used for such diverse purposes as weather forecasting, television broadcast, amateur radio communications, Internet communications and GPS.

The first artificial satellite, launched by Russia (then known as the Soviet Union) in the late 1950s, was about the size of a basketball. It did nothing but transmit a simple Morse code signal over and over. In contrast, modern satellites can receive and retransmit thousands of signals simultaneously, from simple digital data to the most complex television programming.

In a space-age first, two satellites have collided in orbit. On 11 February, 2009, a Russian communications satellite and an American Iridium mobile phone spacecraft smashed into each other, 790 kilometres above Siberia. The cosmic bingle left both write-offs. At least 600 pieces of wreckage have been observed circling the world.

The satellites, both travelling at more than 7 kilometres a second, would have hit at almost right angles. 'It would have been a massive prang,' quoted one source. Orbital traffic control has been impossible because the position of most satellites, until now, could only be plotted to an accuracy of four of five kilometres. A new laser system, developed at a cost of \$50 million with help from the Australian Federal Government and satellite operators, could track objects with an accuracy of a few metres and warn satellite operators when to change course.

The 900 kilogram Russian satellite, Cosmos 2251, was launched in 1991 and ended its working life 10 years ago. The 670 kilogram American vehicle was one of 66 operational Iridium spacecraft relaying satellite-telephone communications. NASA says about 17 000 objects bigger than 10 centimetres, mostly debris from satellites and rockets, circle Earth.

Source: Richard Macey, *The Sydney Morning Herald*, 13 February 2009.

Infra-red radiation is electromagnetic radiation of a wavelength longer than visible light (therefore cannot be seen with the naked eye), but shorter than microwave radiation.

Wireless networks encrypt data before it is broadcast, but there are holes in the system that can be exploited.

connections. A consumer can use a small satellite dish fixed to their property to access the Internet through a service provider who offers satellite connection. Usually, the speed of downloading from the Internet over satellite is significantly faster than uploading. Satellite transmission may be the only alternative for people living in remote rural communities (Figure 1-25).

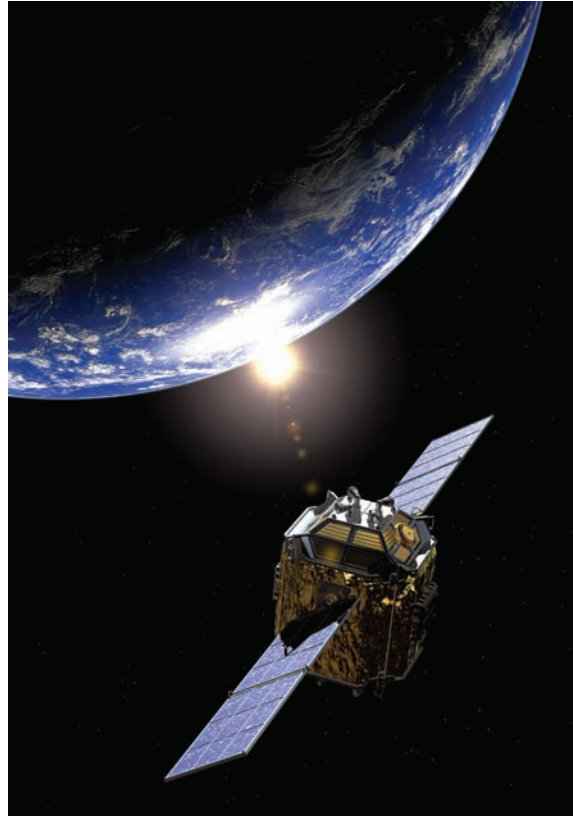


FIGURE 1-25
A mobile communications satellite

Infra-red

Infra-red transmission uses the same technology as the TV and video remote controls. It is usually quite effective over short distances (up to about five metres is good), although the data transfer rate is slow compared to using cables. Many hand-held computers have infra-red ports that can communicate easily with printers or laptops. Thus material can be backed up quite easily and updated from another computer.

Infra-red transmission uses light waves and requires line-of-sight access.

Network security

Networks are vulnerable from attack by hackers and others who may wish to steal information or cause mischief. Networks connected to the Internet are particularly at risk, as are wireless networks. It is essential for networks to have security measures in place to protect them from outside attack.

Physical security measures, such as locks and alarms to warn of intruders, can protect a cabled network to a degree, but it cannot protect it from attack over the Internet. A wireless network must employ additional



FIGURE 1-26

This NASA illustration shows man-made objects within 2000 kilometres of Earth. About 95 per cent of the material is debris.

security, since the nature of radio wave transmission is that its range is often beyond the boundaries of an organisation's property.

A login system that requires usernames and passwords and the installation of a firewall are common security strategies used by most organisations.

Username and passwords

A username is assigned by the network administrator to all authorised users of the network. The username usually is identifiable as belonging to a particular person and can be easily remembered. Usernames are uniquely assigned to users. Passwords are set by the user and should be known only to that user. To maintain high levels of security, user passwords should:

- be at least eight digits long
- include non-alphabetical characters
- not be easily guessed (e.g. a favourite pet's name is not suitable)
- be changed every month.

Some network policies force passwords to be changed on a regular basis, and do not allow passwords to be repeated.

Firewall

A **firewall** is a server and software combination that filters the information coming through an Internet connection into an organisation's internal network. Any packet of data that is flagged by the filters as unwanted is not allowed through.

The filters used by a firewall include examining the IP address of computers that request information from an internal server, blocking all access to certain domain names, banning certain protocols (e.g. file transfer protocol, mail protocol or Telnet protocol) from accessing particular servers, and certain words and phrases included in packets of information.

A firewall can also be used to restrict employees' access to sensitive information. For example, a firewall can be used to stop some personnel from accessing the payroll database.

In buildings, firewalls prevent fire from penetrating into, say, emergency stairwells for up to three hours. Firewalls have no holes and the other side can only be accessed through official doorways.

A server on the LAN can be made available to the Internet using a numbered port (there are 1024 ports available). The firewall can be set to block some network ports from incoming data. By blocking the incoming ports, external users cannot use that port to hack into the local network. Holes are opened through the firewall by unblocking a port. This is done to allow legitimate access to the LAN, such as permitting external users to access the web server. Typical port numbers assigned to services include FTP (port 21), telnet (23), electronic mail (25), gopher (70) and web server (80). If a firewall is not protecting a port, a server set up to accept external connections on that port can be accessed from anywhere on the Internet.

Most firewalls use two separate NICs; one is connected to the internal network and the other to the outside world. Material can only move from one card to the other through the CPU of the server computer that is acting as the firewall. While the data or information is being checked for authenticity, it is also examined for viruses and other malicious codes. Everything that comes in from outside is examined for danger. If it was not specifically requested by someone from inside the network, it is immediately considered dangerous. Sometimes it is not dangerous, but why take unnecessary risks? In an organisation that relies on computers and on the internal networks running, it is bad practice to allow material in that could, potentially, prevent the network from working or allow hostile outsiders to steal data.

Malware protection

Malware refers to malicious software and includes spyware, adware, Trojan horses, worms and viruses. Spyware and adware use cookies to track the Internet sites that a user might visit. Trojan horses can leave your computer open to others to read your personal information by creating backdoor access to your system. Viruses and worms can hijack your system to send multiple emails to others or perform other acts of mischief. Both can use up essential system resources, which may result in the computer freezing.

Network administrators usually require workstations to run virus protection software. The antivirus software is often updated automatically via the network. A firewall is also useful to block malware from sending personal information over the Internet. Anti-adware programs should also be run on workstations.

Encryption

Encryption is the process of translating data into a secret code that can only be read by authorised users. To read an encrypted file, you must have access to a secret key that you use to decrypt the data.

Important data such as credit card details, bank records and medical information should always be stored in encrypted format to protect it from hackers. This becomes especially important if this data is transmitted over the Internet or via radio waves.

Wi-Fi protected access (**WPA** or **WPA2**) is a security protocol for use by wireless LANs. It provides security by encrypting data sent over radio waves so that it is protected during transmission from the sending device to the receiving device. WPA is designed to provide the same level of security to wireless environments as that of a wired network.

Secure websites

Websites that allow financial transactions use the industry standard **hypertext transfer protocol security (https)** as the secure protocol between a client's web browser and the web server, to ensure that a secure connection is established and maintained. Transactions are encrypted and authenticated as they travel across the Internet by industry standard 128-bit SSL encryption to protect the privacy of information. Digital identification certificate technology is based on a trusted certificate authority such as VeriSign Incorporated.

Unencrypted data is referred to as plaintext, while encrypted data is known as ciphertext.



FIGURE 1-27

The digital certificate information for mecu is found by clicking on the locked padlock in the status bar.

Secure sockets layer (SSL) is a cryptographic protocol that provides secure connection on the Internet. When a web browser points to a secured domain, a SSL 'handshake' authenticates the server (website) and the client (web browser). An encryption method is established with a unique session key, and secure transmission can begin.

Every SSL certificate is created for a particular server in a specific domain for a verified business entity. When the SSL handshake occurs, the browser requires authentication information from the server. By clicking the closed padlock in the browser window, the visitor to the website can see the name of the authenticated organisation. In high-security browsers, the authenticated organisation name is prominently displayed and the address bar turns green when an extended validation SSL certificate is detected. If the information does not match or the certificate has expired, the browser displays an error message or warning.

Both Internet Explorer and Firefox will display a locked padlock in the status bar to indicate that you are in a secure site. Other browsers will display https:// in the URL in the website address bar.

Physical design of networks

Networks in medium to large organisations can become very complex, with servers, workstations, printers and cables spread widely throughout the premises. Technical support people need a method of representing the network and all of its different pathways that provides an overview of the connections and allows them to identify and locate equipment.

VCAA will not require students to draw or interpret network diagrams.

A **network diagram** is a schematic method of showing the physical devices and communications lines present in a network. The diagrams use straight lines to represent cables, and icons are used for communications devices. Figure 1-28 shows a network diagram for the John von Neumann Library. You should be able to identify a number of servers, desktop computers, printers, routers, switches and modems. The primary domain controller in this case handles the user logins and also acts as a print server.

Note that the diagram is not based on the plans of the building. This would provide a cumbersome diagram that would be difficult to read. The physical buildings are not important in a network diagram, but it is necessary to identify work areas.

Network diagrams can be drawn using many common graphics packages. The diagram shown in Figure 1-28 was created in TurboCADv5.

Free network diagram software can be downloaded from www.weresc.com/network.php and www.smartdraw.com.

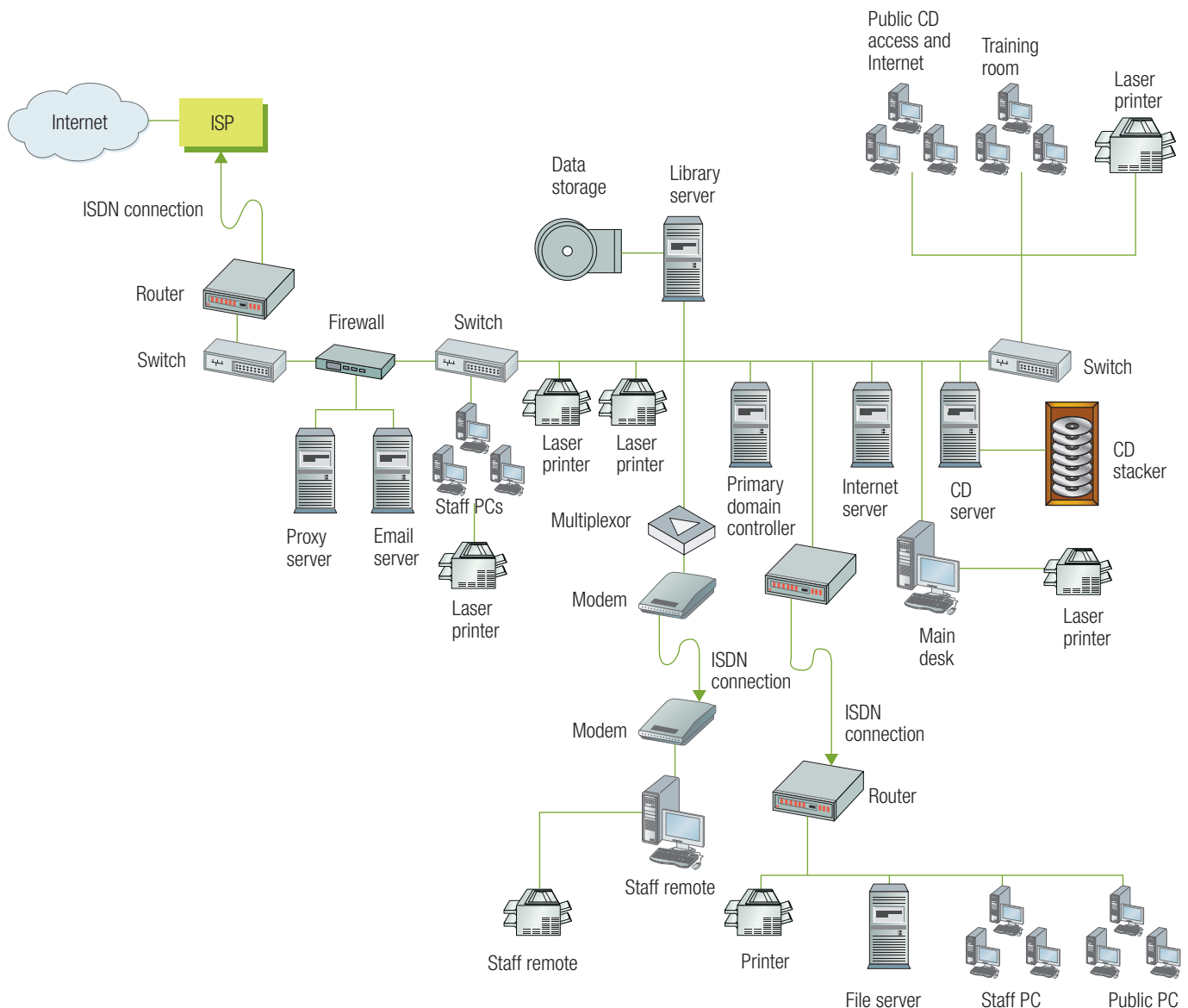


FIGURE 1-28

A network diagram for a library. The diagram shows the communications devices and physical transmission media used in the network.

What you should know

- 1 The **Internet** is a global network that consists of a worldwide collection of networks that connects millions of individuals, organisations, educational institutions, businesses and government agencies.
- 2 A **network** connects computers so that they can share data, information and resources.
- 3 **Resources** are equipment or services that can be used over a network or by a computer.
- 4 Any item that can communicate and can connect to a network is called a **device**.
- 5 The messages that travel over the network are called **network traffic**.
- 6 **Conflict** occurs when two messages are sent by two different devices at virtually the same instant. Neither message is comprehensible.
- 7 **Groupware** is software that allows users to work as a group.
- 8 The advantages of using a network include resource sharing, access to remote services, facilitating communications and data and information sharing.
- 9 A **site licence** allows multiple users of a network to simultaneously use a software package.
- 10 In **timesharing** the processor spends a preset amount of time on a job, then proceeds to the next, and so on.
- 11 **Synchronisation** of data is the process by which all users make certain that they have the latest version of the data to work on.
- 12 **Data duplication** occurs when at least two different users are simultaneously working on their own copy of a data set and independently making changes that they expect others will use.
- 13 Forms of communication over a network include email, chat rooms, messaging and videoconferencing.
- 14 A number of websites have become popular in recent years that support information exchange between online communities. These websites include wikis, blogs, forums and social networking sites.
- 15 A **local area network (LAN)** is a network that connects computers and devices in a limited geographical area.
- 16 **Nodes** are points at which a device connects to the network.
- 17 A **wireless LAN** is a local area network that does not use physical wires or cabling.
- 18 A **wide area network (WAN)** is one in which the user's data travels via a transmission medium not owned by the user.
- 19 The **network architecture** refers to the design of a network, including the computers, devices and media.
- 20 A **client-server network** is one in which one or more computers act as a server, and the other computers on the network request services from the server.
- 21 A **client** is a device that can request data, information or programs from the server, but cannot share its own files or data without putting them on the server.
- 22 A **server** is a machine specially configured to be able to effectively share data or files with other machines on its network.
- 23 **Client-server** is the relationship between these two types of machines.
- 24 A **print server** is a device to which one or more printers are connected and that can accept print jobs from external client computers. The printer server then sends the data to the appropriate printer that it manages.
- 25 A **mail server** is a computer that receives electronic mail and stores it in the recipient's mailbox. Electronic mail can be accepted from a user on the network, or from any other mail server connected to the Internet.
- 26 A **workstation** is a computer attached to a network at which a user can work.
- 27 **Multi-tasking** is where the processor is able to perform more than one task because it only spends a small amount of time on each task before moving to the next and eventually returning to the first task.
- 28 A **peer-to-peer network** is one in which two computers share files directly with each other and both are considered equal in priority.
- 29 **Internet peer-to-peer** allows users to connect to other computers over the Internet and is often used for file sharing.
- 30 An **intranet** is an internal network that uses Internet technologies.
- 31 **Network standards** are the rules by which the physical components of a network are designed and manufactured to make them compatible.

- 32 Protocols** are the rules used to build data packets that are communicated between two devices on a network.
- 33 Ethernet** is a network standard that specifies that no central computer or device on a network should control when data can be transmitted.
- 34** An ethernet **frame** contains packets of information communicated between two network nodes.
- 35 TCP/IP** (Transmission Control Protocol/Internet Protocol) is the protocol used on the Internet.
- 36** A data **packet** contains a chunk of data, the destination address and where it has come from. It often also contains parity information.
- 37 Packet switching** describes the process of breaking a message into several small packets, sending the packets along the best available route, and then reassembling the data at the destination.
- 38** The **802.11 standard** specifies how two wireless devices communicate with each other using radio waves. **Wi-Fi** is short for wireless fidelity and refers to any network based on the 802.11 standard.
- 39** A **network operating system** is the software used to control the network traffic, to build and send packets and to resolve conflicts over network usage.
- 40** Application software designed for use on a network includes electronic mail, web browsers, FTP, chat rooms, instant messaging and videoconferencing.
- 41** A **web browser** allows a user to view pages on the Internet and manages the links used to jump from one document to the next.
- 42** The **URL (uniform resource location)** sent by a requesting browser includes the protocol to be used for the communication, the name of the server hosting the page, and the name of the page being requested.
- 43 Hypertext transfer protocol (http)** is a standard used for transmitting and receiving information on the Internet.
- 44 Web server software** provides documents, images and other resources using the http protocol.
- 45** A **proxy server** sits between the client and the rest of the Internet. When a client's browser requests a page be loaded, the request goes to a proxy server that substitutes its IP address for that of the client. In this way the proxy server ensures the requesting user remains anonymous, allows pages used repeatedly to load from cache rather than from the original source each time, and provides a means for the organisation to block some sites.
- 46 Simple mail transfer protocol (SMTP)** is used on electronic mail servers to handle the sending and receiving of client emails. A **Post Office Protocol (POP3)** server is used to store messages.
- 47 File transfer protocol (FTP)** software enables exchange of the files between computers on the Internet.
- 48 Web software applications** are programs designed for use on a website and include blogging software, forums and wikis.
- 49** A **cross-platform** program runs identically on all machines, regardless of operating system and hardware architecture. Flash and Java are cross-platform applications used to create websites.
- 50** A **network interface card (NIC)** is a computer chip that, in the past, was mounted on a separate add-in card to give the device access to the network and now is built into the motherboard.
- 51** A **wireless access point (AP)** is a central communications device that allows computers and devices to transfer data wirelessly to a wired network.
- 52 Roaming** is the process of moving around a wireless network while maintaining a network connection. A **hot spot** is a location where a user with wireless capability is able to connect to an AP.
- 53** A **switch** only sends the data down the wires directly leading to the device that requested the data. Thus it must store the number of the node for each machine connected to it.
- 54** A **router** determines the best path for packets to follow on their way to their destination. A router is often used to connect two or more LANs.
- 55** A **modem** is a communications device that converts a computer's digital signal into an analog signal.
- 56** A **digital modem** is one that sends and receives data and information to and from a digital connection such as ADSL and broadband cable.
- 57 ADSL** (asymmetric digital subscriber line) provides digital connection over standard copper telephone lines. It is 'asymmetric because the download rate is faster than the upload rate.'

- 58 **Unshielded twisted-pair (UTP) cable** is used to carry signals around a network.
- 59 **Coaxial cable** has a single copper wire surrounded by an insulating material, a braided metal and a plastic outer coating.
- 60 **Fibre-optic cable** consists of numerous thin glass or plastic strands that use light to transmit signals.
- 61 Wireless transmission media include radio waves, microwaves, satellites and infra-red waves.
- 62 **Bluetooth** is a communications standard that uses short-range radio waves. Bluetooth can be used to connect notebook computers, PDAs and smart phones.
- 63 Network security measures include usernames and passwords, firewalls, malware protection and encryption.
- 64 A **firewall** is hardware and software that protects a network's resources from intrusion by users on another network such as the Internet.
- 65 **Malware** refers to software that can potentially impact on the function of a computer or network. It includes spyware, adware, worms and viruses.
- 66 **Wi-Fi Protected Access (WPA or WPA2)** is a security standard that defines how to encrypt data as it travels across wireless networks.
- 67 Hypertext transfer protocol security (https) is a communication standard that ensures a secure connection for financial transactions.
- 68 Secure sockets layer (SSL) is a protocol that provides secure connections on the Internet.
- 69 A **network diagram** is a schematic method of showing the physical devices and communication lines present in a network.

Test your knowledge



Networks

- 1 Define the term *network*.
- 2 What does groupware on a network allow people to do?
- 3 What are the four main advantages in using a network?
- 4 What compelling reason would an organisation use to justify resource sharing?
- 5 What resources, other than printing, can be shared on a network?
- 6 Describe the benefit to an organisation in providing a remote ordering service for customers over the Internet.
- 7 How does file sharing on a network avoid problems associated with data duplication?

Online communities

- 8 Under what circumstances would it be more appropriate to set up a blog rather than a wiki?
- 9 How do wiki sites cope with visitors intent on causing damage or being a nuisance?
- 10 What is a thread in an online forum? How are threads established?
- 11 What type of social networking site would be appropriate for someone who wants share stories, thoughts and photos with friends?

Types of networks

- 12 What are the key differences between WANs and LANs?
- 13 Why are network points called nodes rather than being called computers?
- 14 Explain the difference between a client and a server on a network.
- 15 Describe the roles of the following on a network:
 - (a) database server
 - (b) domain name server
 - (c) proxy server
 - (d) active directory domain controller
- 16 Would a peer-to-peer network be worthwhile on a small network?
- 17 Kazaa was a good example of a peer-to-peer network. It was slower than web servers that use a client-server model. What are the problems with peer-to-peer networks?
- 18 What is a switch?
- 19 Explain why many larger organisations prefer a star topology over a bus topology.

- 20 What advantage does a tree network offer?
- 21 What is an intranet?

Network communication standards

- 22 Why do manufacturers build products based on network standards?
- 23 List four functions included in a network protocol.
- 24 Identify the four components of all ethernet frames.
- 25 Describe how data flows over an ethernet network from the source to the intended destination.
- 26 How does a collision occur on a network? How does ethernet avoid repeated collisions of the same transmissions?
- 27 TCP/IP uses smaller packets than other protocols. Why is this an advantage on the Internet?
- 28 What standard does a Wi-Fi network use?

Network hardware and software

- 29 List a number of tasks undertaken by a network operating system.
- 30 What are the three components of a uniform resource location?
- 31 How does a domain name server assist a web browser in connecting to a website?
- 32 What does the web server software do when it receives a GET request from a client's web browser?
- 33 What are three reasons for using a proxy server on a network that will be used to connect to the Internet?
- 34 Describe the steps involving a SMTP server and a POP3 server that occur when a user on one network sends an email to a user on a different network.
- 35 What do we mean by cross-platform software? Describe an example of cross-platform software.
- 36 What is the role of a network interface card?
- 37 Describe the process of roaming on a Wi-Fi network.
- 38 Why would a café establish a hot spot on the premises?
- 39 What are routers used for?
- 40 How does a modem enable a computer to communicate with a network over a standard telephone line?

- 41 How does a digital modem differ from a dial-up modem?

Transmission media

- 42 Why do new networks use CAT 5 standard cable rather than CAT 3?
- 43 What are some of the disadvantages of using CAT 5 cable? Why is CAT 5 cable used in so many installations?
- 44 Why is fibre-optic cable often used to connect major switches inside buildings as well as between buildings?
- 45 What advantages does wireless networking have over a network that uses physical transmission media?
- 46 What limitation applies to microwave transmissions?
- 47 Why is radio wireless networking preferable to infra-red wireless networking?

Network security

- 48 Why does a wireless network pose a greater security threat than a wired network?
- 49 Recommend a password strategy that an organisation could implement to avoid unauthorised access to their network.
- 50 What are the main purposes of firewalls and how are these purposes achieved?
- 51 What added security feature should wireless networks employ?

Physical design of networks

- 52 What is a network diagram?
- 53 Why is a network diagram not based on the building plans of the organisation?

Apply your knowledge


www.nelsoninfotech.com.au

Nelson Secondary College has decided to update its network. It currently has a small network in the careers area (10 machines). It has another network in the library (23 machines), which is next door to the careers area but not connected to it. There are two computer labs at the other end of the school building about 80 metres away. All three networks work on a client-server model. The school has an Internet connection in the library and two printers on each network.

- 1 (a) Explain why a client-server network would provide a better solution than a peer-to-peer network.
- (b) Provide reasons why the various separate networks around the school should be linked.
- (c) Would you recommend using switches to link the various workgroups, or would you keep the LANs separated by using routers to provide the links? (Consider how many servers there might be and the desire to keep network traffic from adding to conflicts in the library and in the computer labs.)
- 2 (a) List the servers that you would recommend be used on the network, and describe their function.
- (b) The users of the network can be assigned to one of three groups – students, teachers and administrative staff. For each server that you have identified, indicate any limitations on access that you would place on each of the three groups.

It has been suggested that the networks should be connected using fibre-optic cable because, for the most part, it will use the same wall space as the electricity cables and the cables will run parallel for a significant distance.

- 3 (a) Why would it be a problem for UTP (unshielded twisted-pair) cable to run parallel to electricity cables?
- (b) Why is fibre-optic cable a suitable alternative?
- (c) State two other advantages of using fibre-optic cable.
- (d) Would it be easier to use a wireless network instead of fibre-optic cable? Explain.

Nelson SC intends to build a new Middle School campus in the next suburb (three kilometres away).

- 4 The new Middle School is too far away for a cable to be laid between the two campuses. Describe an alternative transmission technology that you would recommend.
- 5 What security strategies would you recommend for the college?

The Outdoor Education Club at the College wishes to establish a website as a means of communicating with past and present members. The website is planned to have several pages that provide information regarding the types of activities performed by the Club, the mission of the Club, membership enquiries, a past members page, and contact details.

- 6 (a) The Club will locate its website on the College's network, making use of the College's hardware, software and Internet connection. What hardware and software specifically belonging to the College's network would the Club's website make use of?
- (b) A member has suggested that the website developer use Flash to make the site more interesting. Describe some of the effects the developer could build into the website using Flash.

The leader of the Club wishes to provide regular information and reports on his trips that members can read if they wish. It would function as a type of journal and will include some photos from the trips.

- 7 (a) What type of site would you recommend?
- (b) What software is required to establish this site?

Another member wishes to create a website that features the Club's major trip to the Grampians. She hopes that members will be able to contribute to the site with comments, pictures and perhaps videos. Members should be able to edit comments made by other members if they think they are incorrect.

- 8 (a) What type of site would you recommend? Why?
- (b) Can access to the site be limited just to members?